

**WEST VALLEY WATER DISTRICT
855 W. BASE LINE ROAD, RIALTO, CA 92376
PH: (909) 875-1804
WWW.WVWD.ORG**

**SPECIAL SAFETY AND TECHNOLOGY COMMITTEE MEETING
AGENDA**

Tuesday, September 15, 2026, 6:00 PM

NOTICE IS HEREBY GIVEN that West Valley Water District has called a meeting of the Safety and Technology Committee to meet in the Administrative Conference Room, 855 W. Base Line Road, Rialto, CA 92376.

BOARD OF DIRECTORS

**Director Daniel Jenkins, Chair
President Kelvin Moore**

Members of the public may attend the meeting in person at 855 W. Base Line Road, Rialto, CA 92376, or you may join the meeting using Zoom by clicking this link: <https://us02web.zoom.us/j/8402937790>. Public comment may be submitted via Zoom, by telephone by calling the following number and access code: Dial: (888) 475-4499, Access Code: 840-293-7790, or via email to administration@wwwd.org.

If you require additional assistance, please contact administration@wwwd.org.

CALL TO ORDER

PUBLIC PARTICIPATION

Any person wishing to speak to the Board of Directors on matters listed or not listed on the agenda, within its jurisdiction, is asked to complete a Speaker Card and submit it to the Board Secretary, if you are attending in person. For anyone joining on Zoom, please wait for the Board President's instruction to indicate that you would like to speak. Each speaker is limited to three (3) minutes. Under the State of California Brown Act, the Board of Directors is prohibited from discussing or taking action on any item not listed on the posted agenda. Comments related to noticed Public Hearing(s) and Business Matters will be heard during the occurrence of the item.

Public communication is the time for anyone to address the Board on any agenda item or anything under the jurisdiction of the District. Also, please remember that no disruptions from the crowd will be tolerated. If someone disrupts the meeting, they will be removed.

PRESENTATIONS

DISCUSSION ITEMS

1. Updates to the Safety and Technology Committee
2. Minutes of the August 3, 2026, Special Safety & Technology Committee Meeting Pg. 5
3. Resolution No. 2026-15 - Approval and Adoption of the SCADA Master Plan Pg. 7
4. Professional Services Agreement with SDI Presence, LLC for an IT Master Plan Pg. 61

ADJOURN

Please Note:

Material related to an item on this agenda submitted to the Board of Directors after distribution of the agenda packet is available for public inspection in the District's office located at 855 W. Base Line Road, Rialto, CA 92376, during normal business hours. Also, such documents are available on the District's website at www.wvwd.org subject to staff's ability to post the documents before the meeting.

Pursuant to Government Code Section 54954.2(a), any request for a disability-related modification or accommodation, including auxiliary aids or services, to attend or participate in the above agendaized public meeting should be directed to the Board Secretary, Brandon Yoshida, at least 72 hours in advance of the meeting to ensure availability of the requested service or accommodation. Brandon Yoshida may be contacted by telephone at (909) 875-1804 ext. 703, or in writing at the West Valley Water District, P.O. Box 920, Rialto, CA 92377-0920.

DECLARATION OF POSTING:

I hereby declare under penalty of perjury, that I am employed by the West Valley Water District, and that the foregoing agenda was posted at the District Office's bulletin boards and the District website at www.wvwd.org on September 10, 2026, by 6:00 pm., in compliance with the provisions of the Brown Act.

Brandon Yoshida

Brandon Yoshida, Board Secretary

Date Posted: September 10, 2026

MINUTES
SPECIAL SAFETY AND TECHNOLOGY SPECIAL COMMITTEE
MEETING
of the
WEST VALLEY WATER DISTRICT
August 3, 2026

I. CALL TO ORDER

Chair Jenkins called the Safety and Technology Committee meeting to order at 6:00 p.m.

Attendee Name	Present	Absent	Late	Arrived
Daniel Jenkins	☒	☐	☐	
Kelvin Moore	☒	☐	☐	
John Thiel	☒	☐	☐	
Linda Jadeski	☒	☐	☐	
Jon Stephenson	☒	☐	☐	
Albert Clinger	☒	☐	☐	

II. PUBLIC PARTICIPATION

Chair Jenkins inquired if anyone from the public would like to speak. No requests were received; therefore Chair Jenkins closed the public comment period.

III. DISCUSSION ITEMS

1. Minutes of the July 6, 2026 Special Safety & Technology Committee Meeting

The Committee approved the minutes as presented.

2. Updates to the Safety and Technology Committee

Director of Technical Services Stephenson reported steady progress on several technology and accessibility projects. The consultant review of the SCADA Master Plan Project is nearing completion, and staff is working to finalize the staff report in August. Tyler has completed its configuration for the Utility Payment API/iPaySmart integration and provided access to iPaySmart, while iPaySmart developers continue reviewing the API documentation and modifying their programming. Staff received seven proposals for the IT Master Plan RFP and is currently reviewing and scoring the proposals. Regarding ADA Title II accessibility requirements, staff recently participated in a six-part webinar series and is developing a plan to meet the April 26, 2028, compliance deadline; preliminary audits have identified deficiencies requiring attention. Staff is coordinating with District departments to identify and address potential impacts associated with the transition of the Westvalleywaterca.gov domain and is working with

Public Outreach and Government Affairs to develop an outreach strategy. Staff is also evaluating a website redesign to align with best practices, improve accessibility and usability, and address accessibility compliance, with the .gov transition and updated branding guidelines further supporting the need for a comprehensive redesign.

IV. ADJOURN

Chair Jenkins adjourned the meeting at 6:30 p.m.

ATTEST:

Brandon Yoshida, Board Secretary

Minutes were approved on September 15, 2026, by the Safety and Technology Committee of the West Valley Water District.



STAFF REPORT

DATE: September 15, 2026

TO: Safety and Technology Committee

FROM: Joanne Chan, Director of Operations

SUBJECT: Resolution No. 2026-15 - Approval and Adoption of the SCADA Master Plan

STRATEGIC GOAL:

Strategic Goal 1 - Manage and Deliver a Safe, Reliable, and Sustainable Water Supply; Objective 1B. Assess, Repair, Replace, Upgrade Aging Infrastructure; and 1E. Ensure Operational Continuity through Comprehensive Physical and Cybersecurity

Strategic Goal 5 – Apply Sound Planning, Innovation, and Best Practices; Objective 5A. Increase Operational Efficiency, Resiliency, and Reliability

MEETING HISTORY:

9/1/26 - Engineering, Operations and Planning Committee

BACKGROUND:

The West Valley Water District (District) operates and maintains critical water infrastructure that relies on Supervisory Control and Data Acquisition (SCADA) systems to monitor and control various treatment, production, distribution, and other operational facilities.

SCADA systems are an integral component of the District's ability to operate its facilities safely and efficiently. As technology continues to evolve and cybersecurity risks increase, maintaining a reliable, secure, resilient, and sustainable SCADA environment is essential to supporting operational continuity, regulatory compliance, system reliability, and long-term infrastructure planning.

To address these needs, the District undertook the development of a comprehensive SCADA Master Plan. The purpose of the Master Plan is to evaluate the District's existing SCADA environment, identify current and future operational and technological needs, establish recommended standards and strategies, and develop a prioritized framework for future improvements and investments.

DISCUSSION:

The SCADA Master Plan provides a structured approach for addressing the District's current SCADA needs while establishing a framework for future improvements. Adoption of the Plan will assist the District in coordinating SCADA-related planning and investment decisions and in maintaining consistency among future projects.

The Plan also provides a foundation for addressing evolving cybersecurity requirements, technological changes, system reliability, equipment lifecycle needs, and operational requirements. Periodic review and updates will allow the District to maintain the Plan as conditions, technology, regulatory requirements, and District priorities change.

Staff is therefore recommending that the Board approve and adopt Resolution No. 2026-15 and accept the SCADA Master Plan as the District's planning document and strategic framework for future SCADA development and modernization. Resolution No. 2026-15 is attached as **Exhibit A**, with the SCADA Master Plan attached to the Resolution.

FISCAL IMPACT:

There is no direct fiscal impact associated with adoption of the SCADA Master Plan.

The Master Plan identifies potential future improvements, upgrades, and investments; however, adoption of the Plan does not authorize expenditures or commit the District to any specific project or procurement. Any future projects or expenditures identified in the Master Plan will be subject to separate review, funding authorization, and approval in accordance with applicable District policies and procedures.

REQUESTED ACTION:

Staff recommends that the Committee forward a recommendation to the Board of Directors to:

1. Approve and adopt Resolution No. 2026-15, approving and adopting the District's SCADA Master Plan; and
2. Authorize the General Manager, or his or her designee, to periodically review and recommend updates to the SCADA Master Plan, as necessary, consistent with District policies and procedures.

Attachments

[Exhibit A - Resolution 2026-15.pdf](#)

EXHIBIT A

RESOLUTION NO. 2026-15

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT APPROVING AND ADOPTING THE SCADA MASTER PLAN

WHEREAS, the West Valley Water District ("District") operates and maintains critical water infrastructure supported by a Supervisory Control and Data Acquisition ("SCADA") system; and

WHEREAS, the District recognizes the importance of a reliable, secure, resilient, and sustainable SCADA system to support the safe and efficient operation of its facilities, regulatory compliance, operational continuity, cybersecurity, and long-term infrastructure planning; and

WHEREAS, the District undertook the development of a comprehensive SCADA Master Plan to evaluate the existing SCADA environment, identify operational and technological needs, establish recommended standards and strategies, and develop a prioritized framework for future SCADA improvements, upgrades, integration, cybersecurity, and lifecycle management; and

WHEREAS, the completed SCADA Master Plan provides recommendations and a long-term roadmap for the District's SCADA infrastructure, including system architecture, communications, hardware and software, cybersecurity, controls, instrumentation, system integration, reliability, redundancy, lifecycle management, and implementation priorities; and

WHEREAS, the Board of Directors has reviewed the completed SCADA Master Plan and finds that the Plan provides a reasonable and appropriate framework for guiding the District's future SCADA-related planning, design, procurement, improvements, and capital investments.

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT DOES HEREBY RESOLVE AS FOLLOWS:

SECTION 1. The Board hereby approves and adopts the SCADA Master Plan as presented to the Board and attached hereto as Exhibit "A".

SECTION 2. The Board hereby authorizes the General Manager, or his or her designee, to take any and all actions necessary to implement the SCADA Master Plan as the District's planning document and strategic framework for the future development, modernization, operation, maintenance, cybersecurity, and management of its SCADA systems.

SECTION 3. This Resolution shall be effective as of the date of adoption.

SECTION 4. The Recitals set forth above are incorporated herein and made an operative part of this Resolution.

SECTION 5. The General Manager, or his or her designee, is hereby authorized and directed to periodically review and recommend updates to the SCADA Master Plan as necessary to reflect changes in technology, operational requirements, cybersecurity risks, regulatory requirements, infrastructure needs, and District priorities. Material amendments to the Plan shall be presented to the Board for consideration and approval when required by District policy.

SECTION 6. Approval of the SCADA Master Plan does not, by itself, authorize expenditures, contracts, procurements, construction projects, or other commitments not previously approved by the Board. Individual projects and expenditures identified in the Plan shall be brought forward for authorization in accordance with applicable District policies and procedures.

SECTION 7. Pursuant to the California Environmental Quality Act (“CEQA”) and State CEQA Guidelines, the approval of the SCADA Master Plan is not subject to CEQA under State CEQA Guidelines Section 15060(c)(3) because it is not a “project” as defined by State CEQA Guidelines Section 15378. There is no potential for the activity to result in either a direct physical change in the environment or a reasonably foreseeable indirect physical change in the environment. In addition, approval of the SCADA Master Plan is also exempt from CEQA pursuant to State CEQA Guidelines Section 15061(b)(3). CEQA applies only to projects which have the potential for causing a significant effect on the environment. It can be seen with certainty that there is no possibility that the approval of the SCADA Master Plan may have a significant effect on the environment. Therefore, the activity is not subject to CEQA and no further environmental review is necessary.

SECTION 8. If any section, subsection, sentence, clause, or phrase of this Resolution is for any reason held invalid or unenforceable, such decision shall not affect the validity of the remaining portions of this Resolution.

PASSED, APPROVED AND ADOPTED this ____ day of September 2026.

KELVIN MOORE
President
Board of Directors
West Valley Water District

ATTEST:

Brandon Yoshida
Board Secretary

CERTIFICATION

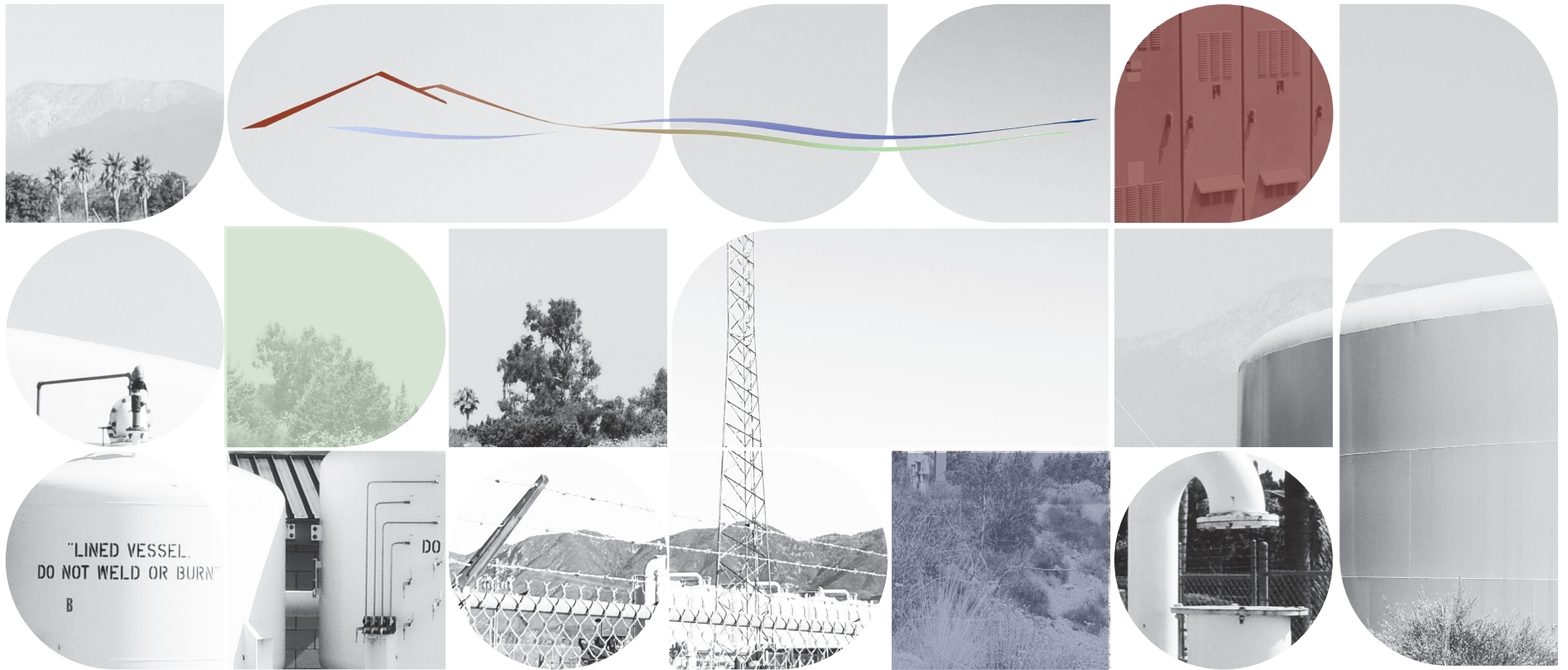
I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing Resolution No. 2026-15 was duly adopted by the Board of Directors of the West Valley Water District at a regular meeting held on September ____, 2026, by the following vote:

AYES:	BOARD MEMBERS:
NOES:	BOARD MEMBERS:
ABSENT:	BOARD MEMBERS:
ABSTAIN:	BOARD MEMBERS:

Dated: September ____, 2026

Brandon Yoshida
Board Secretary

EXHIBIT A



08
19
26

PREPARED FOR

WEST VALLEY WATER DISTRICT

SCADA MASTER PLAN

PREPARED BY

Josh Choe
Advanced Integration & Controls

Stephen Goldsworth, CISSP
JEGO Systems





TABLE OF
CONTENTS

1. Introduction	7	3.4.6 ICS Cybersecurity System Architecture Design	15
1.1 Purpose.....	7	3.4.7 Wireless Backhaul Communication System	15
1.2 Document Organization	7	3.4.8 Project Summary and Estimates for Long- and Short-Term Planning.....	15
1.3 Companion Documents	7	4. Current Environment	15
2. Executive Summary.....	9	4.1 Supply & Distribution System (HQ)	15
3. Project Overview	11	4.1.1 Architecture	15
3.1 Purpose of This Project	11	4.1.2 Asset List	15
3.2 Project Participants	11	4.1.3 SCADA	15
3.2.1 District Stakeholders	11	4.1.4 Infrastructure	17
3.2.2 AIC Stakeholders.....	11	4.1.5 Telemetry & Communications.....	19
3.2.3 JEGO Systems Stakeholders	11	4.1.6 Field	19
3.2.4 Applied Technologies Group (ATG) Stakeholders	11	4.1.7 PLC & Process Control.....	19
3.3 SCADA Master Plan Vision	13	4.2 Water Filtration Facility System (OPR)	19
3.3.1 Goals and Objectives	13	4.2.1 Architecture	19
3.3.2 Key Benefits	13	4.2.2 Asset List	19
3.4 Project Approach	13	4.2.3 SCADA	19
3.4.1 Request for Records, Drawings, and Background Information	13	4.2.4 Infrastructure	21
3.4.2 Kickoff Meeting/Ideas Exchange Workshop	13	4.2.5 Telemetry & Communications	23
3.4.3 Key Stakeholders Identification and Analysis	13	4.2.6 Field	23
3.4.4 Evaluation of Existing ICS Assets	13	4.2.7 PLC & Process Control	25
3.4.5 System Gap Analysis.....	15	4.3 Summary Review Highlights.....	25
		4.3.1 Documentation Summary Review Highlights	25
		4.3.2 Configuration Summary Review Highlights	25

5. Needs Assessment Summary 27

5.1 Needs Assessment Workshops 27

5.1.1 NA Workshop 1 – SCADA & Infrastructure..... 27

5.1.2 NA Workshop 2 – IT Support & Infrastructure Standards..... 27

5.1.3 NA Workshop 3 – Field & PLC 27

5.2 Summary of Needs 27

5.2.1 SCADA 27

5.2.2 Infrastructure..... 31

5.2.3 Networking & Telemetry 31

5.2.4 Field 33

5.2.5 PLC 35

6. Cybersecurity Evaluation 37

6.1 Security Controls Gap Assessment 37

6.2 Assessment Summary 37

6.2.1 Maturity Level Descriptions 37

6.2.2 Maturity Level Results Table..... 39

6.2.3 Maturity Level Results by Function 41

6.2.4 Maturity Level Results by Category 41

6.3 Assessment Findings 43

6.3.1 Security Control Functions..... 43

6.3.2 Governance Summary 45

6.3.3 Identification Summary..... 45

6.3.4 Protection Summary 45

6.3.5 Detection Summary 45

6.3.6 Response Summary 45

6.3.7 Recovery Summary 47

6.4 Baseline Security Policy 47

6.5 Cybersecurity Requirements Specification (CRS)49

6.6 Response & Recovery Plan49

6.6.1 Incident Response Communication Pathways49

6.6.2 Incident Response & Recovery Workflow49

7. System Gap Analysis 51

7.1 SCADA 51

7.1.1 Software Reliability, Redundancy & Long-Term Support 51

7.1.2 Historian Data Analysis Tools & Data Integration..... 51

7.1.3 System Alarming & Notifications 53

7.1.4 System Staffing & Training 53

7.1.5 User Interface 53

7.2 Infrastructure..... 53

7.2.1 SCADA Platform, Backups & Standardization 53

7.2.2 Platform Environment, Monitoring & Operational Redundancy 55

7.2.3 Core Networking 55

7.2.4 Telemetry..... 57

7.2.5 PLC & Process Control 57

8. System Design Criteria59

8.1 Software Standards59

8.1.1 Software Documentation Standards 59

8.1.2 SCADA59

8.1.3 Historian & Data Integration59

8.1.4 Notifications & Alerting 61

8.1.5 Administration & Maintenance Independence 61

8.2 Hardware Standards 61

8.2.1 General Hardware Standards 61

8.2.2 Virtual Servers, Storage & Platform 63

8.2.3 Monitoring & Notification 63

8.2.4 Redundancy 63

8.2.5 Telemetry65

8.3 Field Enclosure Standards 65

8.4 Programming Standards 65

8.4.1 General PLC Programming Standards 65

8.4.2 Program Architecture & Organization 65

8.4.3 I/O Processing Standards 67

8.4.4 Alarm Logic Standards 67

8.4.5 Process Control Standards 67

8.4.6 Communications & Data Exchange 67

8.4.7 Program Documentation & Version Control 67

8.4.8 Testing, Commissioning & Change Management 67

8.5 Cybersecurity Standards 67

8.5.1 Overview 67

8.5.2 Key Considerations 67

8.5.3 General Cybersecurity Design Standards 67

9. Project Recommendations..... 69

9.1 Short-Term Projects (S) 69

9.1.1 S-1 Radio Communication Infrastructure Upgrade 69

9.1.2 S-2 HQ System Core Infrastructure Upgrades 71

9.1.3 S-3 HQ SCADA Application Modernization 73

9.1.4 S-4 OPR WFF Network Segmentation & Resiliency Improvements 77

9.1.5 S-5 PLC Standard Documentation79

9.1.6 S-6 SCADA Standard Documentation79

9.2 Mid-Term Projects (M) 81

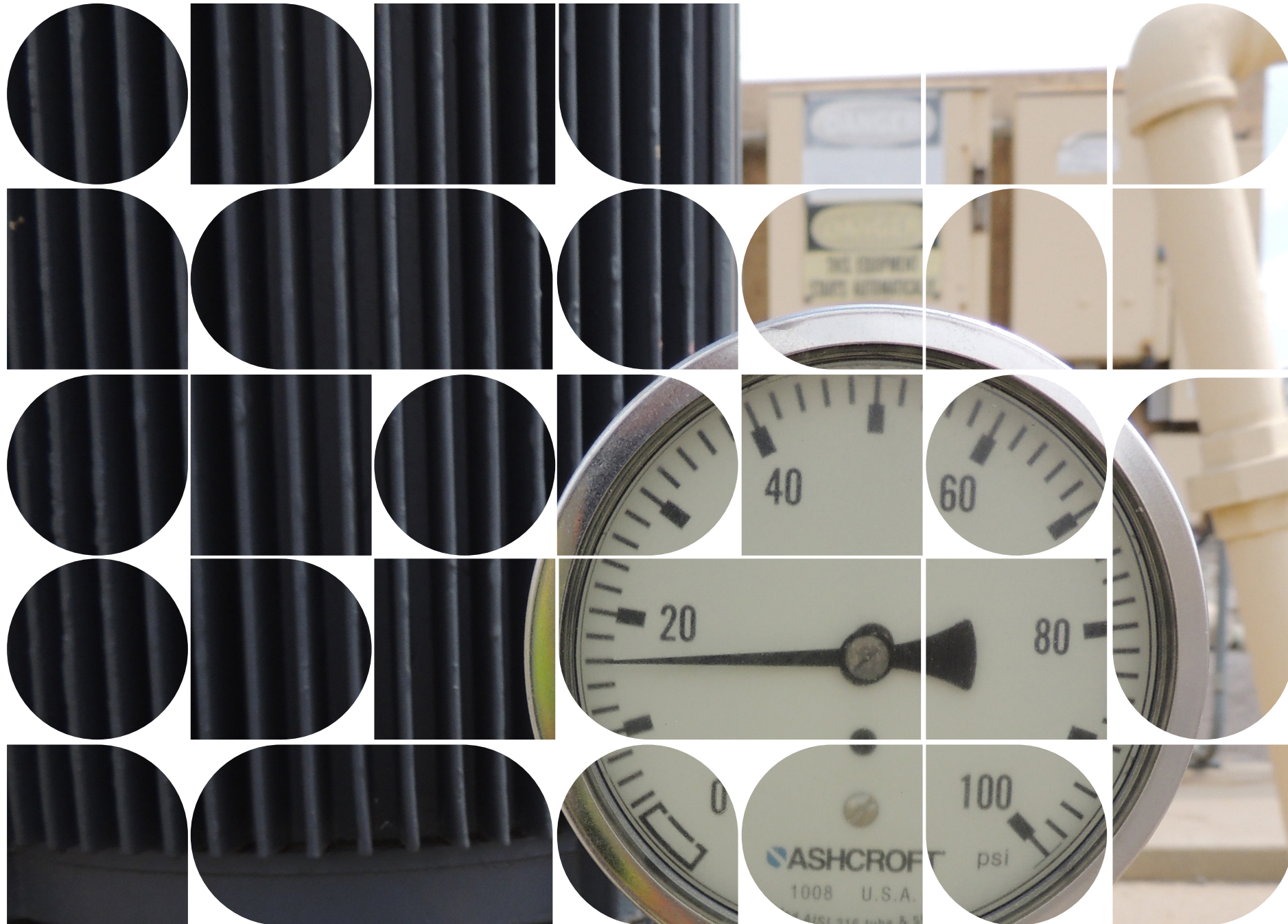
9.2.1 M-1 Cybersecurity Control Gap (Re)Assessment 81

9.2.2 M-2 Response & Recovery Plan Integration83

9.3 Long-Term Projects (L)85

9.3.1 L-1 Remote Site Panel, PLC & SCADA Upgrade Program 85

10. Companion Documents 89



1 | INTRODUCTION

1.1 PURPOSE

The West Valley Water District (District) commissioned this SCADA Master Plan (SMP) to provide a strategic roadmap for the modernization of its Industrial Control System (ICS) environment. The plan establishes a long-term vision for improving system reliability, operational efficiency, cybersecurity, maintainability, and resilience while supporting the District's future operational needs.

The SCADA Master Plan documents the District's existing control system environment and identifies current challenges and opportunities. It also establishes design criteria and standards and recommends a phased implementation strategy to guide future investments in SCADA, networking, communications, cybersecurity, and process control systems.

1.2 DOCUMENT ORGANIZATION

This report is organized into the following sections:

Executive Summary – Summarizes the assessment findings, key recommendations, and implementation strategy.

Project Overview – Describes the project objectives, participants, vision, and overall planning approach.

Current Environment – Documents the District's existing SCADA, network, communications, and control system infrastructure.

Needs Assessment – Summarizes stakeholder input and operational requirements identified during workshops.

Cybersecurity Evaluation – Presents the cybersecurity assessment results and recommended security framework.

System Gap Analysis – Identifies deficiencies between the current environment and the District's desired future state.

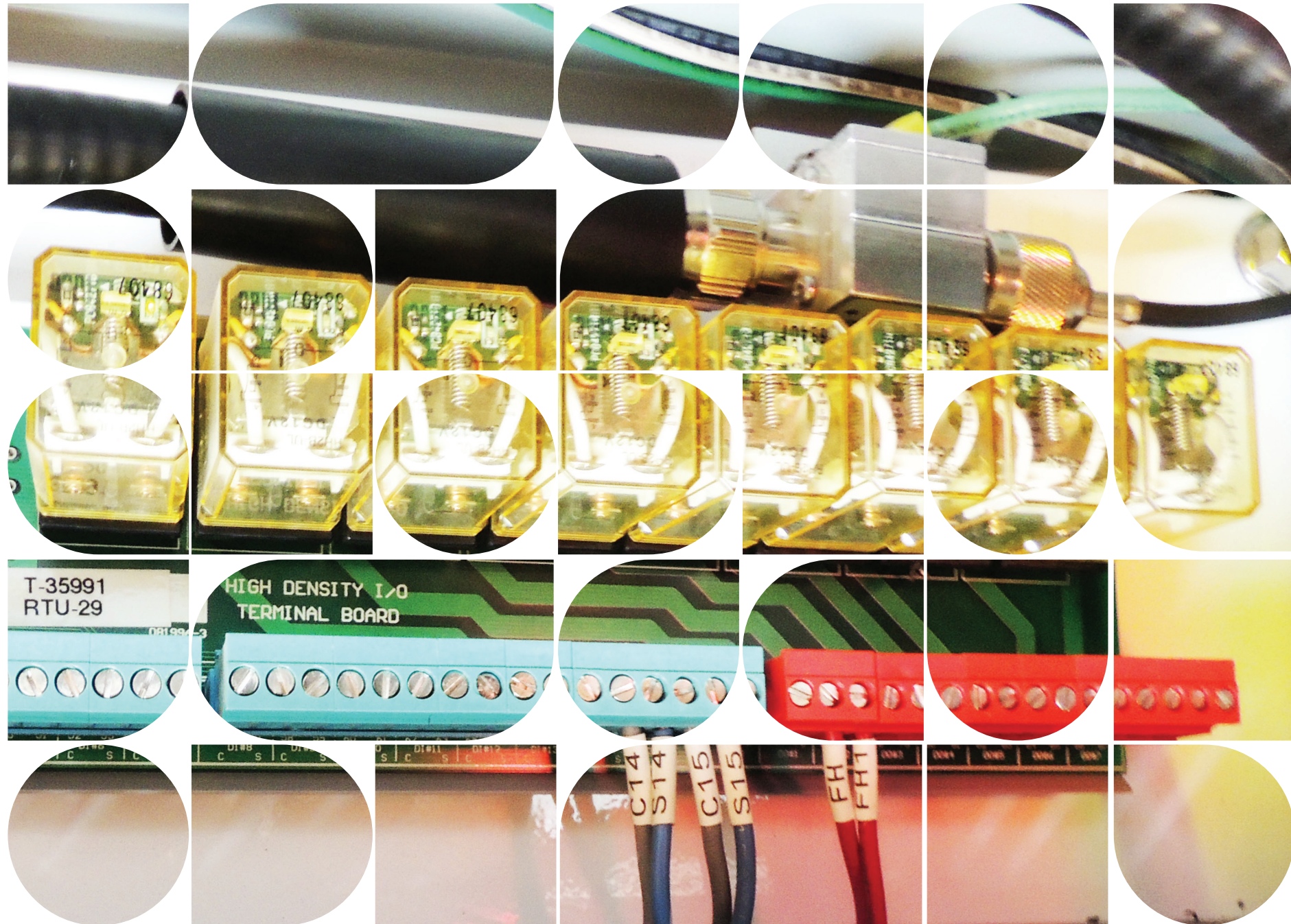
System Design Criteria – Establishes engineering and operational standards to guide future projects.

Project Recommendations – Prioritizes implementation projects into short-, mid-, and long-term initiatives.

Companion Documents – Lists the supporting documents developed as part of the SCADA Master Plan.

1.3 COMPANION DOCUMENTS

The SCADA Master Plan is supported by a series of companion documents that provide detailed technical information, standards, policies, drawings, inventories, and implementation resources. These documents are maintained separately from the Master Plan and are intended to serve as living documents owned and maintained by the District. As systems, policies, standards, and operational requirements evolve, these companion documents should be reviewed and updated to reflect current conditions.



2 | EXECUTIVE SUMMARY

The District's existing SCADA infrastructure - which supports water supply, treatment, and distribution operations serving over 98,000 customers - has reached a point where aging equipment, evolving cybersecurity threats, and growing operational demands require a comprehensive, forward-looking plan. This document is the product of that effort.

The SMP was developed by Advanced Integration & Controls (AIC), in partnership with Jego Systems (JEGO) and Applied Technologies Group (ATG). Over the course of this engagement, the project team conducted extensive data collection, stakeholder interviews, and numerous workshops across multiple District departments including operations, engineering, maintenance, IT, and management. Site visits were performed at all District facilities to document existing system configurations, assets, and network architectures. This collaborative process ensured that every recommendation in the plan is informed by the District's actual operating conditions and priorities.

Through this process, the team identified critical areas requiring attention across the

District's SCADA environment, including end-of-life communication infrastructure, aging core infrastructure components, legacy SCADA software requiring platform migration, and cybersecurity gaps relative to the NIST Cybersecurity Framework (CSF). The detailed findings from the current environment assessment, needs analysis, cybersecurity evaluation, and gap analysis are presented in Sections 4 through 7 of this document.

Based on these findings, the SMP presents a prioritized set of project recommendations organized into short-term (S-#), mid-term (M-#), and long-term (L-#) categories.

Short-term projects - designed to begin as soon as possible and be completed within two years - address the most pressing needs: replace the legacy radio communication infrastructure with a modern, distributed IP-based network (S-1); upgrade HQ core infrastructure including servers, storage, and networking (S-2); migrating the HQ SCADA application from Wonderware InTouch to AVEVA System Platform (S-3); implement network segmentation and resiliency improvements at the OPR Water Filtration

Facility (S-4); and establish standardized PLC and SCADA documentation (S-5 and S-6).

Mid-term projects include a cybersecurity controls gap reassessment (M-1); integration of the response and recovery plan into District operations (M-2).

The long-term project recommendation is a comprehensive Remote Site Panel, PLC, and SCADA Upgrade Program (L-1), which will replace legacy Tesco LIQ PLCs and aging field control panel infrastructure at approximately 37 remote sites with modern Allen-Bradley CompactLogix controllers. This program is structured in two phases: a mid-term phase addressing the highest-priority sites based on equipment condition, operational criticality, and cybersecurity exposure, followed by a long-term phase covering the remaining sites - with the full program to be completed within ten years after the SCADA Master Plan.

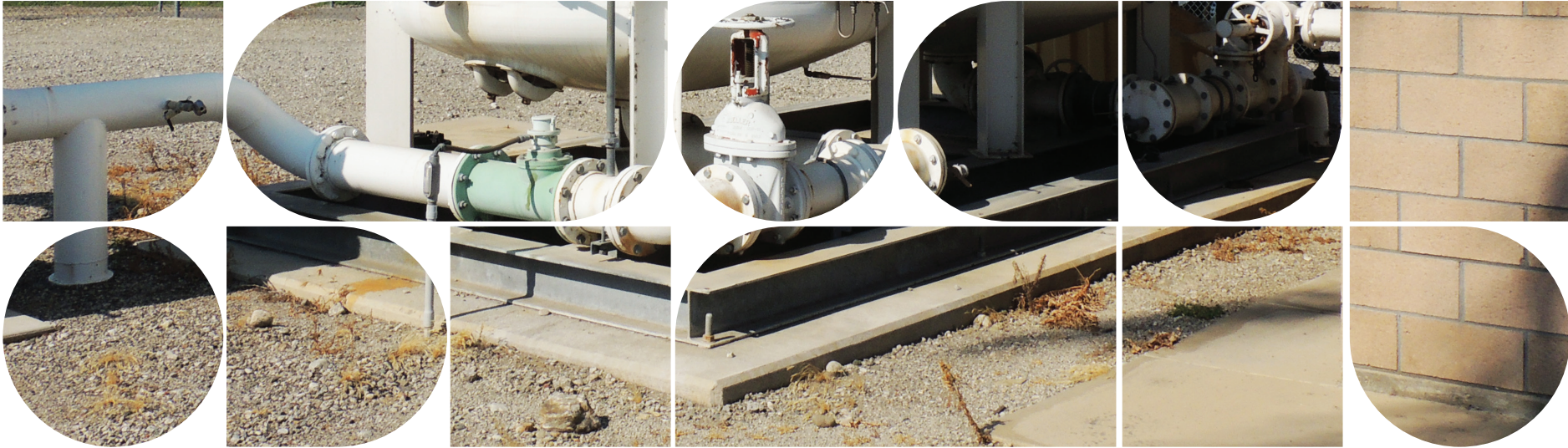
Beyond the project recommendations, this plan delivers a comprehensive set of system design criteria covering software standards, hardware standards, field enclosure standards, programming standards, and cybersecurity standards. These criteria provide the District with a consistent framework for evaluating and

implementing future ICS projects, ensuring each investment aligns with the overall modernization strategy and industry best practices.

The SMP also includes a cybersecurity evaluation chapter with a baseline security policy, cybersecurity requirements specification, and an incident response and recovery plan. These components provide the District with the policy framework and procedural guidance necessary to protect critical water infrastructure against evolving cyber threats while maintaining operational continuity.

With this master plan in hand, the District is empowered to make informed decisions about which projects require comprehensive plans and specifications and which can be swiftly implemented through professional

service procurements. The SMP is intended to serve as a living document with a multi-year planning horizon that may be updated regularly as the District's needs evolve, technologies advance, and projects are completed. Ultimately, this plan provides the strategic foundation for the District to modernize its ICS infrastructure efficiently, securely, and sustainably - ensuring reliable water service to the community for years to come.



3 | PROJECT OVERVIEW

3.1 PURPOSE OF THIS PROJECT

This section describes the project that produced the SCADA Master Plan: its purpose, the District and consultant personnel who participated, the long-term vision that guided the work, and the task-by-task approach followed from the initial records request through project scoping and estimating.

The purpose of this project is to define the target state of the District's SCADA environment and the sequence of work required to reach it. The SMP establishes a common vision across Operations, Engineering, and Information Technology; sets design criteria for SCADA, network, communication, cybersecurity, and process control systems; and translates those criteria into scoped and budgeted projects spanning a ten-year planning horizon. The plan is intended to serve as a working reference for capital budgeting, scope development, and consistent evaluation of future ICS investments.

3.2 PROJECT PARTICIPANTS

A Core Team of District staff was involved in each step along the way, along with our subject matter experts ("SME") from AIC, JEGO Systems, and ATG; they provided invaluable assistance and input. The project was also supported by a group of stakeholders that provided input on District operations and user needs. We truly appreciate the efforts, commitment, and excellence in execution the

Core Team and Stakeholders demonstrated. We believe the SMP has a strong foundation as a result of this participation. A list of the various stakeholders involved in any significant capacity is detailed below.

3.2.1 District Stakeholders

- › Joanne Chan, Director of Operations
- › Jon Stephenson, Director of Technical Services (IT)
- › Albert Clinger, Business System Manager (IT)
- › Nathan Cao, IT Administrator
- › Robert Ramirez, IT Specialist
- › Ben Jarrell, E I & C Specialist
- › John Martin, E I & C Specialist
- › Paul Andrews, E & I Technician
- › Brian Grubert, Lead Water Treatment Operator
- › Joe Schaack, Chief Water Systems Operator – Production
- › Jonathan Barfield, Water Production Operator III
- › Socorro Pantaleon, Public Outreach & Government Affairs Manager
- › Mary Jo Hartley, Senior Public Outreach & Government Affairs Rep
- › William Fox, Chief Financial Officer
- › Gustavo Gutierrez, Finance Manager
- › Rudy Olguin, Chief Water Systems Operator – Distribution
- › Sergio Granda, Chief Water Systems Operator – Treatment
- › Haydee Sainz, Human

Resources & Risk Manager

- › Yolanda Ramirez, Human Resources Specialist
- › John Thiel, General Manager
- › Linda Jadeski, Assistant General Manager
- › Rocky Welborn, Director Of Engineering
- › Rosa Gutierrez, Senior Engineer

3.2.2 AIC Stakeholders

- › Kevin Ford, PMP, Lead Project Manager
- › Adam Simmons, Supporting Project Manager
- › Josh Choe, Lead SCADA & Data Collection, Network & Telemetry Engineering
- › David Estelle, PE, Lead PLC HW & SW Technologies, Supporting SCADA & Data Collection
- › Joe Vang, Supporting PLC HW & SW Technologies
- › AJ Cottingham, PE, Supporting PLC HW & SW Technologies
- › Michael Prosser, Collaborative Delivery (Internal)
- › Zach Meitz, Lead Field Activities
- › Jesus Lopez, Supporting Field Activities
- › Alex Valdez, Supporting Field Activities
- › Alfonso Ducreux, Lead I&C Engineer
- › Brian Damelio, Supporting I&C Engineer
- › Ben Green, Lead AI & Alternative Technologies

3.2.3 JEGO Systems Stakeholders

- › Stephen Goldsworth, CISSP, Lead Cybersecurity & Network Engineering

- › Webster Jessup, Supporting Cybersecurity & Network Engineering
- › Michael Goldsworth, Cybersecurity Analyst

3.2.4 Applied Technologies Group (ATG) Stakeholders

- › James Ronnow, Supporting Network & Telemetry
- › Jeff Gillam, Supporting Network & Telemetry

3.3 SCADA MASTER PLAN VISION

As the District seeks to transition its proprietary Industrial Control System (ICS) into a secure, flexible, and future-ready environment, the need for a comprehensive SMP has never been more pressing. Modernizing the current infrastructure, will ensure reliable service for over 98,000 customers, protect critical water resources, enhance cybersecurity, and support long-term organizational growth. Our proposal addresses these challenges directly, guiding the District towards an adaptive, vendor-neutral ICS that aligns with best practices and industry standards like the NIST Cyber-security Framework.

3.3.1 Goals and Objectives

The primary goal of the SMP is to define a roadmap for the District SCADA Systems to guide future development of infrastructure, processes, organization, and staff with the intent of having systems that support and facilitate water operations, and are supportable by District resources. As part of the planning

process, the team reviewed the District’s environment, identified existing technology gaps and areas for standardization, and developed specific design criteria and project recommendations that will help achieve operational and business efficiencies. This plan provides the District with a set of SCADA projects and cost estimates that will assist with meeting its overall goals, which include the following:

- › Develop a roadmap for the SCADA system to guide future development of infrastructure, processes, organization, and staff.
- › Provide SCADA systems that support and facilitate water operations.
- › Promotes a SCADA system that is supportable by District resources.
- › Results in a common cross-departmental vision for the future of the District’s SCADA and related systems.
- › Develops enterprise alignment regarding major SCADA System projects that require substantial District investments.
- › Helps to create a better understanding of the organization’s SCADA data needs and developing system capabilities to meet those needs.
- › Results in a living planning document with a multi-year planning horizon that may be updated regularly.
- › Identifies projects and activities needed to implement the Plan.
- › Provides a basis for budgetary investments for the next ten years.
- › Provides guidelines for phasing of projects and activities.

- › Defines a clear migration path for replacement of obsolescent technologies for system growth and upgrades.
- › Provides direction for achieving and maintaining SCADA system security requirements for the water sector.

3.3.2 Key Benefits

The SMP presents a cohesive, forward-looking blueprint for the District’s ICS evolution. The SMP includes not only architecture recommendations, asset inventories, and cybersecurity frameworks but also proposed policies, procedures, disaster recovery plans, and detailed project outlines. With this master plan in hand, the District is empowered to confidently decide which projects require comprehensive plans and specifications, and which can be swiftly implemented through professional service RFPs—thus reducing unnecessary costs and accelerating modernization.

3.4 PROJECT APPROACH

3.4.1 Request for Records, Drawings, and Background Information

Information on the existing system was requested and provided by the District. Examples included system and site drawing sets, network and architecture diagrams, operation and maintenance manuals, process control narratives, and software application and configuration files.

- 3.4.1.1.1 Activities and Deliverables
 - › Documentation Request

- › Documentation Workshop
- › Configuration Request
- › Configuration Workshop

3.4.1.2 Reference Information

The information provided in the previous task was utilized to form a baseline of the existing control system environment. This baseline was captured in summarized reports that detail the findings to support subsequent gap analysis activities.

- 3.4.1.2.1 Activities and Deliverables
 - › Documentation Review
 - › Documentation Summary Report
 - › Configuration Review
 - › Configuration Summary Report

3.4.2 Kickoff Meeting/ Ideas Exchange Workshop

This collaborative kickoff meeting with the District established the stakeholders and intended approach to developing the District’s SMP.

- 3.4.2.1.1 Activities and Deliverables
 - › Project Kickoff Meeting
 - › Project Kickoff Summary Document

3.4.3 Key Stakeholders Identification and Analysis

A needs assessment matrix was developed using information gathered during workshops, shadow sessions, and interviews with key stakeholders across multiple disciplines within the District.

- 3.4.3.1.1 Activities and Deliverables
 - › Planning Workshop (Initial)
 - › Department-Specific Workshops
 - › Stakeholder Shadow Sessions and Interviews
 - › Final Review Workshop
 - › Needs Assessment Summary
 - › Surveys (Optional)

3.4.4 Evaluation of Existing ICS Assets

Data collection was used to gather missing information that could not be obtained in previous task activities, and involved multiple site visits to gather system and asset details using various capture methods. This information was used to generate an existing system architecture and asset list to represent the existing system, allow for infrastructure assessments, and support gap analysis activities in the subsequent task.

3.4.4.1 Data Collection

- 3.4.4.1.1 Activities and Deliverables
 - › Data Collection Scope Workshop
 - › Data Collection Schedule Workshop
 - › Data Collection Stakeholder Selection Workshop
 - › Data Collection Plan Summary Document
 - › Onsite Data Collection
 - › Data Collection Summary Document

3.4.4.2 Existing Architecture and Asset List

- 3.4.4.2.1 Activities and Deliverables

- › Develop Preliminary Asset Lists
- › Asset List Review Workshop 1
- › Finalize Asset List
- › Asset List Review Workshop 2
- › Develop Preliminary Existing Architecture
- › Document Architecture Assumptions
- › Architecture Review Workshop 1
- › Finalize Existing Architecture
- › Architecture Review Workshop 2

3.4.4.3 System Infrastructure Assessments

- 3.4.4.3.1 Activities and Deliverables
 - › Perform Field and Core Infrastructure Assessments
 - › Field and Core Infrastructure Assessment Review Workshop
 - › Finalize Field and Core Infrastructure Assessment

3.4.5 System Gap Analysis

The existing system configuration details, infrastructure assessments, asset lists, system architecture, and the needs assessment information were used to identify gaps and obstacles that need to be addressed in order to transition from the current system to one that meets the District’s current and future expectations.

- 3.4.5.1.1 Activities and Deliverables
 - › Preliminary Gap Analysis
 - › Gap Analysis Review Workshop
 - › Finalized Gap Analysis

3.4.6 ICS Cybersecurity System Architecture Design

To ensure the design incorporates modern Cybersecurity standards, a controls gap assessment is performed to ensure attention in the design to fundamental security requirements relevant to the water sector. The existing architecture was reviewed, and a Cybersecurity requirements summary was generated along with a proposed architecture and design recommendations, and followed by the development of a Disaster Recovery Plan (DRP) and relevant baseline policies and procedures to meet the security objectives.

3.4.6.1 Cybersecurity Controls Gap Assessment

3.4.6.1.1 Activities and Deliverables

- › (Controls) Gap Assessment Workshops
- › (Controls) Gap Assessment Analysis and Finalization

3.4.6.2 Architecture Review

3.4.6.2.1 Activities and Deliverables

- › Preliminary and Final Architecture Review Workshops
- › Architecture and Configuration Review Documentation

3.4.6.3 Cybersecurity Requirements Summary

3.4.6.3.1 Activities and Deliverables

- › Develop and Review Cybersecurity Requirements Summary

3.4.6.4 Disaster Recovery Planning

3.4.6.4.1 Activities and Deliverables

- › Workshops and Draft Plan for Incident Response and Recovery (IRR)
- › Finalized IRR Plan

3.4.6.5 Policy and Procedure Development

3.4.6.5.1 Activities and Deliverables

- › Workshops and Development of Baseline Policies and Procedures
- › Finalize Baseline Policies & Procedures

3.4.7 Wireless Backhaul Communication System

This task supports the development of a robust, reliable, and high-performance wireless communication system by utilizing SME's in the field of industrial wireless communications.

3.4.7.1.1 Activities and Deliverables

- › RF Theoretical Modeling
- › RF Theoretical Modeling Workshop
- › RF Field Survey
- › RF Field Survey Results Workshop

3.4.8 Project Summary and Estimates for Long- and Short-Term Planning

Three primary groups of project duration types were generated along with detailed scopes of work, bill of materials, and drawings (where applicable), and budgetary estimates.



4 | CURRENT ENVIRONMENT

Record requests, configuration reviews, and onsite visits to all District facilities were used to inventory the existing control system environment and produce the architecture drawings and asset lists referenced throughout this section. The results establish the documented baseline against which the needs assessment, cybersecurity evaluation, and gap analysis in Sections 5 through 7 are measured.

The District operates two distinct core SCADA systems, each with its own SCADA, network, and process control infrastructure. The Supply and Distribution System (HQ) comprises largely legacy components, while the OPR Water Filtration Facility system was recently upgraded. Each system is detailed below.

4.1 SUPPLY AND DISTRIBUTION SYSTEM (HQ)

The Supply and Distribution System SCADA System, also known as the HQ System, is located at the District's Headquarters. It provides monitoring and control capabilities for wells, boosters, and other geographically distributed process sites that make up the HQ Supply and Distribution System.

4.1.1 Architecture

The HQ System Architecture was provided to the District as Companion Document B.

4.1.2 Asset List

The HQ System Asset List was provided to the District as a separate document.

4.1.3 SCADA

The SCADA system consists of redundant SCADA servers (SCADA Server 1 and SCADA Server 2). The SCADA application integrates with Windows Active Directory for user authentication and authorization, supported by two domain controllers (Domain Controller 1 and Domain Controller 2).

SCADA clients access the system through Remote Desktop Services (RDS) sessions via an RDS/Broker server. Access is provided from physical SCADA workstation clients as well as remote devices, such as tablets and laptops, through a Remote Access Gateway. The Historian collects process data from the active primary SCADA server (SCADA Server 1 or SCADA Server 2). An Engineering Workstation (Engineering Workstation 1) supports local application development and other administrative activities.

The SCADA system polls the majority of remote-site PLCs over serial radio telemetry. In addition, a microwave communication link between the HQ system and the OPR system supports local SCADA client access at each facility—OPR hosts an HQ SCADA client, and HQ hosts an OPR SCADA client.

4.1.3.1 Major SCADA Assets

4.1.3.1.1 Hypervisor Servers

- › Hypervisor 1

› Hypervisor 2

4.1.3.1.2 Virtual Machines

- › Remote Access Gateway
- › Domain Controller 1
- › Domain Controller 2
- › RDS/Broker Server
- › SCADA Server 1 (& TopView Server 1)
- › SCADA Server 2 (& TopView Server 2)
- › Historian
- › Engineering Workstation

4.1.3.1.3 SCADA Client Workstations

- › Client 1 (Physical Workstation)
- › Client 2 (Physical Workstation)
- › Client 3 (Physical Workstation)

4.1.3.1.4 Alarm Notification Devices

- › SMS Modem 1
- › SMS Modem 2

4.1.3.1.5 NTP Servers

- › Time Machine NTP Server

4.1.3.1.6 Backup Storage

- › Network Attached Storage (NAS) Device

4.1.3.2 Software

4.1.3.2.1 SCADA Platform

The SCADA platform is Wonderware InTouch.

4.1.3.2.2 Historian Platform

The SCADA Historian platform is Wonderware Historian.

4.1.3.2.3 Alarm Notification Platform

The alarm notification platform is Exele TopView, and uses SMS as the primary notification method.

4.1.3.2.4 User Interface

The HQ SCADA clients are physical workstations in various locations running remote desktop sessions. District staff also use tablets and laptops to host remote sessions as they move throughout the various SCADA sites.

4.1.3.2.5 Software Standards

The SCADA standard is a legacy example consistent with prior integrator’s standard, but District does not have a documented standard reflecting the current system.

4.1.3.2.6 Reporting & Analytics

The current process for producing process data reports involves using Excel add-ins (Historian Client Tools) to retrieve SCADA data from the Historian. This data is then manually combined with information collected in manual sample reports to generate the required state reports. Additional Historian Client tools, such as Trend, are utilized within the SCADA application as well as during troubleshooting and process monitoring activities.

4.1.4 Infrastructure

The core infrastructure components supporting SCADA are largely legacy devices that have exceeded their supported lifecycles and are no longer actively supported by the

manufacturers. While the computing and storage components offer limited redundancy, they lack features for automatic recovery in the event of hardware failures. This limitation is primarily due to the use of a free version of the hypervisor software, which does not include the richer recovery and high-availability features available in licensed versions.

4.1.4.1 Computing & Storage

The system consists of two Dell PowerEdge hypervisors, each hosting multiple virtual machines that support various SCADA components. The hypervisor platform is a legacy, unlicensed version of VMware vSphere (ESXi); as a result, the hypervisors operate independently and do not share computing or storage resources. The VMs hosted by each hypervisor are listed below:

4.1.4.1.1 Computing

4.1.4.1.1.1 Hypervisor 1 VM Inventory

- › Domain Controller 1
- › RDS/Broker Server
- › SCADA Server 1 (& TopView Server 1)
- › Historian

4.1.4.1.1.2 Hypervisor 2 VM Inventory

- › Remote Access Gateway
- › Domain Controller 2
- › SCADA Server 2 (& TopView Server 2)
- › Engineering Workstation 1

4.1.4.1.2 Storage

The computing (VM) storage is hosted on the individual hypervisors. There is a network attached storage (NAS) device that is used for locally backing up configurations and historical data. Creation and storage of specific configurations is a manual process; however, IT utilizes at hybrid cloud solution (Rubrik) to maintain backups of SCADA VMs.

4.1.4.2 Core Networking

The system includes network segmentation that separates components into distinct network zones based on similar security profiles and the communication requirements needed to support essential SCADA functions. There is no redundancy in any of the core networking components.

4.1.4.2.1 Network Segmentation

The following network segments have been provisioned for the HQ system. For network asset assignments, refer to the architecture drawings and the asset lists included as Companion Document A & B.

4.1.4.2.1.1 ICS Management Zone

- › SCA-MGMT: Out-of-Band/Side-band Management Network
- › FW-MGMT: Firewall Management Network
- › DMZ-MGMT: DMZ Management Network

4.1.4.2.1.2 ICS Level 3.5 Zone

- › DMZ-UPS: UPS Network
- › DMZ-NTP: NTP Network

- › DMZ-RA: Remote Access Network
- › DMZ-SMS: Alarm Notification SMS Network
- › DMZ-VOIP: Alarm Notification VOIP Network

4.1.4.2.1.3 ICS Level 3 Zone

- › SCA- STOR: Storage Network
- › SCA-NMS: Monitoring Network
- › SCA-DC: Domain Controller Network
- › SCA-RDS: Remote Desktop Network
- › SCA-CLI: Client Workstation Network

4.1.4.2.1.4 ICS Level 2 Zone

- › SCA-ESXI: Hypervisor Network
- › SCA-SRV: SCADA Network
- › SCA-PRNT: Printer Network

4.1.4.2.1.5 ICS Level 1 Zone

- › PRCS-PLC: Process Network

4.1.4.2.2 Firewalls

The SCADA firewall is a nonredundant Palo Alto device that serves as a primary enforcement boundary between the process control system and untrusted networks outside the OT environment. It provides the DMZ networks that host the GPS Network Time Protocol (NTP) device and the alarm notification SMS modems. The firewall also supports secure remote access via VPN to enable mobile device connectivity and third-party support activities.

4.1.4.2.3 Routers

The main router is a nonredundant Cisco device that maintains a trunk connection to the SCADA firewall. It provisions the majority of the OT networks, including the DMZ hosting the Remote Access Gateway VM, and enforces traffic-shaping policies between OT networks. The router also maintains trunk connections to various distribution and access switches, which connect SCADA system sites and components to the respective process control networks.

4.1.4.2.4 Switches

The core switch is a nonredundant Cisco device that maintains a trunk connection to the main router. The hypervisors, along with other devices such as printers, storage devices, and workstation clients, are connected to this core switch.

4.1.4.3 Environmental & Utilities

The core infrastructure and primary SCADA components are installed in a networking rack adjacent to the operator workstations in the SCADA control room. The room is environmentally controlled, and relatively clean although somewhat cramped given the multiple uses of this area. There are uninterruptable power supplies (UPS) in the rack that are presumed to be in good working order and capable of providing an acceptable amount of runtime to bridge the gap between when the utility power is dropped and the local site generator starts providing backup power. The infrastructure environment is not currently monitored, nor is the infrastructure components themselves.

4.1.4.3.1 Location & Physical Environment

- › Core SCADA infrastructure and operator workstations are co-located in a single control room.
- › The room is environmentally controlled, relatively clean, but somewhat cramped.
- › Multiple uses of the area has increased clutter or congestion.

4.1.4.3.2 Backup Power

- › Uninterruptible Power Supplies (UPS) are present in the rack.
- › Presumed operational, providing enough runtime until local generator backup activates.
- › No confirmation of UPS testing or monitoring is mentioned.

4.1.4.3.3 Monitoring

Neither the environmental conditions (temperature, humidity) nor the infrastructure components themselves are actively monitored.

4.1.5 Telemetry & Communications

The primary communications topology for the HQ System is an RF network, consisting of licensed 900 MHz serial radios located at HQ and most remote sites. A communication tower at HQ serves as the main connection point for the majority of sites, while several other sites use repeaters at adjacent locations to link back to HQ. The primary communication protocol is Data Express+, a proprietary protocol used by the Tesco PLCs. In addition, a few Allen-Bradley PLCs at the Fluidized Bed

Reactor (FBR) and Arsenic plant are polled by SCADA using Rockwell’s Ethernet/IP protocol.

4.1.5.1.1 Licensed 900MHz Serial Radios

- › Licensed serial GE MDS Master radio located t HQ. Access point to majority of remote sites
- › FCC Call Sign: WNEP898

4.1.5.1.2 Unlicensed 900MHz Ethernet Radio

- › GE MDS iNET-II remote radio links to Arsenic Plant Access Point. Arsenic Plant Access point also link to Well 1A, Well 2A and Well 5A

4.1.5.1.3 Unlicensed 900MHz Ethernet Radio

- › GE MDS iNET-II Access Point links Meridian TO, Well 6 and Well 11.

4.1.5.1.4 Licensed 23GHz Dragonwave Point-to-Point Radios

- › High speed point-to-point backbone link between HQ and OPR
- › FCC Call Sign: WSDG600 (HQ), WSDG601 (OPR)

4.1.6 Field

Field equipment across the HQ System remote sites encompasses instrumentation, motor control, and control panel infrastructure. A comprehensive field assessment was conducted across all HQ System sites, revealing widespread aging infrastructure dating from the late 1980s through the early 2000s. The majority of field enclosures, wiring, and components require modernization to meet current safety codes, operational reliability

standards, and cybersecurity requirements. The following subsections summarize the existing field conditions by category.

4.1.6.1 Instrumentation

Field instrumentation across the HQ System sites primarily consists of level transmitters, flow meters, and pressure transducers used to monitor reservoir levels, well production, and booster pump station operations. Several sites utilize PMC level transducers and Siemens flow meter transmitters. The assessment identified that many field wire connections lack proper labeling, and at some sites flow meters are not wired into the control panels, limiting SCADA monitoring capabilities. Sites such as Well 5A and Well 54 have instruments that are disconnected or not communicating with the PLC, resulting in stations operating only in hand control mode. Existing instrumentation at most sites is functional but requires improved wiring documentation and reconnection to the SCADA system where gaps exist.

4.1.6.2 Motor Control

Motor control at HQ System sites is managed through a combination of Motor Control Centers (MCCs) and individual starters. The majority of MCC equipment was manufactured by TESCO, RSE Sierra, Pacific Electric, Benjamin Electric, and Siemens, with installations dating from 1987 through 2012. MCC sections house PLC equipment in dedicated telemetry or pump control sections within the lineup. Several well sites, including Well 5A, Well18A, Well42, and

Well 54, currently operate only in hand control mode due to communication failures or control system disconnects. The District has expressed the desire to return automatic SCADA-based pump control functionality at these sites. Variable Frequency Drives (VFDs) have been retrofitted at some locations such as Well 54 for well pump and booster pump operation. Motor control upgrades should be coordinated with PLC replacements to ensure full integration with the modernized SCADA system.

4.1.6.3 Control Panels & Electrical Distribution

The HQ System field control panels are predominantly TESCO wallmount and MCC-style enclosures constructed of galvanized steel with ANSI 61 Gray finish. Enclosure types include NEMA Type 3R (outdoor rated), Type 3RX (stainless steel), Type 12, and Type 1 (indoor). Wallmount enclosures are typically 28”H x 22”W x 12”D with 24”H x 18”W backpans, while MCC-mounted configurations utilize 70”H x 22”W or 70”H x 33¼”W backpanels.

The field assessment identified several critical findings common across the majority of sites. No UL508A short circuit current rating validation was performed at every assessed site. Multiple sites have 480VAC and 120VAC present in the same enclosure without proper voltage separation barriers or exterior warning labels. The majority of enclosures lack cooling fans, intrusion switches, enclosure lighting, and Surge Protection Devices (SPDs). Many backboards and door gaskets are degrading,

and several enclosures show external rust and corrosion. Dust, rodent droppings, and spider webs are present in numerous enclosures and can contribute to degradation of electrical components. Coaxial cables are not properly grounded at most sites, and lightning arrestors are absent at many locations.

Backup power is typically provided by 12VDC chargers with 12V 18Ah sealed lead-acid batteries. Battery replacement intervals are inconsistent, with some batteries dating to original installation. A few sites use Marathon Power UPS systems (1500VA) rated only to 104°F, which is inadequate for outdoor operating environments and should be transitioned to charger/battery configurations. Ethernet switches are absent at the vast majority of sites; only a small number have N-Tron 104Tx unmanaged switches, which should be replaced with managed switches for cybersecurity and diagnostics.

4.1.7 PLC & Process Control

The PLCs that make up the process control system primarily run as standalone programs for wells, boosters, and intertie sites. Some peer-to-peer communication is supported by a PLC (RTU-99) located at HQ. Additionally, the FBR plant has dedicated PLCs that operate independently and are not part of the larger HQ System.

4.1.7.1 PLC Platform

The primary PLC platform is Tesco LIQ’s; there are multiple different generations of Tesco PLC’s, all of which are legacy models that are

proprietary in nature – only Tesco Controls services and provides Tesco LIQ PLC’s.

4.1.7.2 Software Standards

The PLC standard is a legacy example consistent with prior integrator’s standard (Tesco Controls), but District does not have a documented standard reflecting the current system.

4.1.7.3 Process Control

The process control narratives for the PLCs are provided as Companion Document D.

4.2 WATER FILTRATION FACILITY SYSTEM (OPR)

The Water Filtration Facility (WFF) SCADA System, also referred to as the OPR System, is located at the Oliver P. Roemer Water Filtration Facility (OPR WFF). It provides monitoring and control capabilities for OPR WFF. The system has not been officially turned over to the District at the time the SMP was written.

4.2.1 Architecture

The OPR System Architecture was provided to the District as a separate document

4.2.2 Asset List

The OPR System Asset List was provided to the District as a separate document

4.2.3 SCADA

The SCADA system consists of redundant SCADA server virtual machines, AVEVA I/O Server 1 and AVEVA I/O Server 2. The SCADA application

integrates with Windows Active Directory for user authentication and authorization, supported by two domain controller virtual machines (Domain Controller 1 and Domain Controller 2).

SCADA clients access the system through ThinManager, using two redundant ThinManager servers (ThinManager Server 1 and ThinManager Server 2) and Remote Desktop Services (RDS) sessions hosted on RDS Server 1 and RDS Server 2. Client access is provided from physical SCADA workstations in the operations building control room, as well as panel-mounted PCs located throughout the plant areas. While not currently implemented, there are plans to deploy a local Wi-Fi network to support tablet-based client access as operators move throughout the plant.

Process data is collected by two redundant Tier 1 Historians (Historian 1 and Historian 2), which receive data from the active primary SCADA server. A Tier 2 PI Historian located in the DMZ is intended to receive data from the Tier 1 Historians. An Engineering Workstation is used for local application development and other administrative functions.

Several assets reside within the DMZ networks; however, it is unclear whether these systems are currently operating as originally designed. This includes the SolarWinds server and the RADIUS authentication server, as detailed in the Major SCADA Assets section. A vCenter virtual machine is also present to manage the hypervisor platform.

The SCADA system polls the majority of plant-area PLCs over a local Ethernet LAN. In addition, a microwave communication link between the HQ system and the OPR system enables local SCADA client access at each facility—OPR hosts an HQ SCADA client, and HQ hosts an OPR SCADA client.

4.2.3.1 Major SCADA Assets

4.2.3.1.1 Hypervisor Servers

- › Dell VRTX Chassis (4-Node)
- › Hypervisor 1
- › Hypervisor 2
- › Hypervisor 3

4.2.3.1.2 Virtual Machines

- › DMZ – ITAA Secure Gateway
- › DMZ – Jump Host
- › DMZ – AV/Malware Management
- › DMZ – Patch Manager
- › DMZ – Historian 3 (Tier 2 PI Historian)
- › DMZ – Radius Authentication Server 2
- › DMZ – SIEM Server
- › Domain Controller 1
- › Domain Controller 2
- › RDS Server 1
- › RDS Server 2
- › Historian 1
- › Historian 2
- › TopView Alarm Notification 1
- › TopView Alarm Notification 2
- › ThinManager Server 1

- › ThinManager Server 2
- › AVEVA I/O (SCADA) Server 1
- › AVEVA I/O (SCADA) Server 2
- › Engineering Workstation
- › Report Server
- › Solarwinds Server
- › Radius Authentication Server
- › vCenter Server

4.2.3.1.3 SCADA Client Workstations

- › Client 1 (Physical Workstation)
- › Client 2-3 (Future Physical Workstations)
- › Client 4 (Future Physical Workstation at HQ)

4.2.3.1.4 Alarm Notification Devices

- › Voice Modem 1
- › Voice Modem 2
- › SMS Modem 1
- › SMS Modem 2

4.2.3.1.5 NTP Servers

- › SyncServer NTP Server

4.2.3.1.6 Backup Storage

- › None identified

4.2.3.2 Software

4.2.3.2.1 SCADA Platform

- › The SCADA platform is AVEVA System Platform.

4.2.3.2.2 Historian Platform

- › The SCADA Historian platform is Wonderware Historian.

4.2.3.2.3 Alarm Notification Platform

- › The alarm notification platform is Exele TopView, and uses SMS and Voice (VOIP) as the primary notification methods.

4.2.3.2.4 User Interface

The SCADA clients are physical workstations located in the operations building control room at the OPR facility; note that there is only one workstation client currently, but there are plans for up to five. There are also panel mount PC’s throughout the plant areas, and there are plans for WiFi tablet clients.

4.2.3.2.5 Software Standards

The SCADA standard is consistent with prior integrator’s standard, but District does not have a documented standard reflecting the current system. However, the District prefers this standard over the legacy HQ standard. A project regarding documenting this standard has been included in the project recommendations section of this SMP.

4.2.3.2.6 Reporting & Analytics

There is a reporting server VM (Report Server 1) in the architecture but it is not clear what the exact process is for producing reports.

4.2.4 Infrastructure

The core infrastructure components supporting the SCADA system are modern devices that remain within their supported lifecycles and are actively supported by their respective manufacturers, as expected for a

recently designed and commissioned system. Computing and storage components provide both hardware and software redundancy and incorporate automatic recovery features in the event of hardware failures. In contrast to the HQ System, this enhanced resiliency is largely attributable to the use of a licensed hypervisor platform, which provides advanced high-availability and recovery capabilities not available in free versions.

4.2.4.1 Computing & Storage

The system consists of a Dell VRTX 4-node (blade) chassis with 3 Dell blade server hypervisors set up in a cluster and hosting multiple virtual machines that support various SCADA components. The hypervisor platform is a modern, licensed version of VMware vSphere (ESXi); as a result, the hypervisors can share computing and storage resources. The VMs hosted by the hypervisor cluster are listed below:

4.2.4.1.1 Computing

4.2.4.1.1.1 Hypervisor 1,2,3 (Cluster) VM Inventory

- › DMZ – ITAA Secure Gateway
- › DMZ – Jump Host
- › DMZ – AV/Malware Management
- › DMZ – Patch Manager
- › DMZ – Historian 3 (Tier 2 PI Historian)
- › DMZ – Radius Authentication Server 2
- › DMZ – SIEM Server
- › Domain Controller 1
- › Domain Controller 2

- › RDS Server 1
- › RDS Server 2
- › Historian 1
- › Historian 2
- › TopView Alarm Notification 1
- › TopView Alarm Notification 2
- › ThinManager Server 1
- › ThinManager Server 2
- › AVEVA I/O (SCADA) Server 1
- › AVEVA I/O (SCADA) Server 2
- › Engineering Workstation
- › Report Server
- › Solarwinds Server
- › Radius Authentication Server

4.2.4.1.2 Storage

The computing (VM) storage is hosted on the hypervisors. It is unclear what the current backup strategy or location is for critical configurations and VMs.

4.2.4.2 Core Networking

The system includes network segmentation that separates components into distinct network zones based on similar security profiles and the communication requirements needed to support essential SCADA functions. There is semi-redundancy in some of the core networking components, namely the core switch (stacked), but not in the firewall (traffic-shaping device for OT networks).

4.2.4.2.1 Network Segmentation

The following network segments have been provisioned for the OPR system. For network asset assignments, refer to the architecture drawings and the asset lists included as Companion Document A & B.

4.2.4.2.1.1 ICS Level 4/5 Zone

- › SCA-CORP: Business Network Zone

4.2.4.2.1.2 ICS Management Zone

- › SCA-MGMT: Out-of-Band/Side-band Management Network

4.2.4.2.1.3 ICS Level 3.5 Zone

- › SCA-DMZ: DMZ Network

4.2.4.2.1.4 ICS Level 2/3 Zone

- › SCA-SCADA: SCADA Network

4.2.4.2.1.5 ICS Level 1 Zone

- › SCA- PCN: Process Network
- › SCA-RIO: Process RIO Network

4.2.4.2.2 Firewalls

The SCADA firewall is a nonredundant Fortinet device that serves as the primary enforcement boundary between the process control system and untrusted networks outside the OT environment. There are currently no connections north of the firewall to the District’s IT network or the internet. However, a temporary cellular device is connected to the WAN interface of the SCADA firewall and is believed to provide internet access for the integrator’s remote development activities. The SCADA firewall provides the DMZ networks that host the various DMZ VMs. The firewall is intended (per

the design) to support secure remote access via VPN to enable mobile device connectivity and third-party support activities. The firewall contains the traffic-shaping policies between the OT networks, with the exception of the SCADA to Process (PLC) network. In lieu of a routing policy rule for SCADA to PLC traffic, the SCADA Servers (AVEVA I/O Server 1 and AVEVA I/O Server 2) are dual-homed with interfaces on both the SCADA (SCA-SCADA) and PLC (SCA-PCN) VLANs.

4.2.4.2.4 Switches

The core switch is a semi-redundant Cisco device (2 stacked switches) that maintains a trunk (LAG) connection to the SCADA firewall. The hypervisors, along with other devices such as workstation clients and alarm notification modems, are connected to this core switch. The router also maintains trunk connections to various distribution and access switches, which connect SCADA system plant PLCs and components to the respective process control LANs.

4.2.4.3 Environmental & Utilities

The core infrastructure and primary SCADA components are installed in a network rack located in a dedicated room adjacent to the control room in the operations building at OPR; there is a PLC control panel in this room as well. The room is environmentally controlled and generally clean; however, there is a noticeable accumulation of construction dust and debris on many of the rack-mounted components. Uninterruptible power supplies (UPS) are

installed within the rack and are presumed to be in good working order, providing sufficient runtime to bridge the gap between a utility power loss and the startup of the local backup generator. At present, the infrastructure environment does not appear to be actively monitored, nor is there monitoring in place for the infrastructure components themselves.

4.2.4.3.1 Location & Physical Environment

- › Core SCADA infrastructure is located in a dedicated networking closet that also contains a PLC control panel.

4.2.4.3.2 Backup Power

- › Uninterruptible Power Supplies (UPS) are present in the rack.
- › Presumed operational, providing enough runtime until local generator backup activates.
- › No confirmation of UPS testing or monitoring is mentioned.

4.2.4.3.3 Monitoring

Neither the environmental conditions (temperature, humidity) nor the infrastructure components themselves are actively monitored.

4.2.5 Telemetry & Communications

The primary communications topology for the OPR System consists of segmented Ethernet local area networks (LANs) inter-connecting plant-level process controls with the supervisory SCADA layer. The primary protocol within the plant network is Rockwell Ethernet/IP, used for PLC-to-SCADA polling

across the Process Control Network (PCN) and Remote I/O (RIO) segments. A licensed 23 GHz point-to-point microwave link provides the primary wide-area backhaul between the OPR facility and HQ, supplemented by PSTN voice and cellular SMS modems for alarm notification and communication redundancy.

4.2.5.1 Plant Process Control Network (PCN & RIO)

- › SCADA Process Network carries Ethernet/IP polling traffic between AB ControlLogix L84E PLCs and the AVEVA I/O Servers located in the Operations Building.
- › PLC Remote I/O carries traffic between the PLC and remote I/O within each filter building process area.
- › AB Stratix 5400 managed switches are installed at Filter Building 1 (FB1) and Filter Building 2 (FB2), providing Layer 2 segmentation between the PCN, RIO VLANs, and supporting CIP device management.
- › A Device Level Ring (DLR) topology provides redundant field-level Ethernet connectivity for instrumentation on process Trains 1, 2, and 3, including existing IPS1 and EPS1 I/O. A dedicated DLR redundancy cable path is provisioned alongside each ring segment.

4.2.5.2 Licensed 23 GHz Microwave Backhaul

- › DragonWave 23ES30SFC point-to-point licensed microwave radios provide the primary WAN backbone link between the OPR facility and HQ (Main Office).

- › This high-speed licensed link carries SCADA supervisory data, historian replication, and domain services traffic between the two primary facilities.

4.2.5.3 Wireless (Local)

- › A Cisco 9800-L-C Wireless LAN Controller / Access Point (WVWD-WFF-OPR-OB-WAP-1) provides local Wi-Fi coverage within the operations building and adjacent areas.
- › District-imaged mobile devices (iPads) connect to the wireless network using RADIUS authentication (UF2A login) for secured access to SCADA thin-client sessions via ThinManager.

4.2.5.4 Alarm Notification – Voice & SMS

- › Two Grandstream voice modems (WVWD-WFF-OPR-OB-MDM-1 and MDM-2) on the SCADA VLAN (VLAN 30) provide PSTN voice call-out capability integrated with the Exele TopView alarm notification platform.
- › Two Multitech SMS modems (WVWD-WFF-OPR-OB-MDM-3 and MDM-4) on the SCADA VLAN provide cellular text message (SMS) notification as a secondary alarm delivery channel.

4.2.5.5 Time Synchronization (NTP)

- › A Microchip SyncServer NTP Server (WVWD-WFF-OPR-OB-NTP-1) provides authoritative network time synchronization for all SCADA, domain, and control system components on the SCADA VLAN, ensuring consistent event and alarm timestamping across the system.

4.2.6 Field

Field equipment at the OPR Water Filtration Plant encompasses instrumentation, motor control, and control panel infrastructure dedicated to the plant’s treatment processes. Unlike the distributed remote sites of the HQ System, the OPR System’s field equipment is concentrated within the plant footprint and connected via Ethernet local area networks. The following subsections summarize the existing field conditions at the OPR facility.

4.2.6.1 Instrumentation

The OPR Water Filtration Plant utilizes process instrumentation typical of a water treatment facility, including flow meters, level transmitters, pressure transducers, turbidimeters, chlorine analyzers, and pH sensors distributed across the treatment process areas. Instrumentation is wired to local control panels and communicates with the plant’s Allen Bradley ControlLogix PLCs via the Ethernet/IP network. Instrument calibration and maintenance practices should be documented as part of the overall SMP to ensure measurement accuracy and regulatory compliance.

4.2.6.2 Motor Control

Motor control at the OPR Water Filtration Plant is managed through Motor Control Centers located within the plant buildings. The MCC equipment supports the operation of treatment process pumps, blowers, and other motorized equipment. Motor starters, variable frequency drives, and soft starters are used throughout the plant as appropriate for

the application. Motor control is integrated with the Allen Bradley ControlLogix PLC system, enabling automatic process control and SCADA monitoring of all motor-driven equipment. Any future motor control upgrades should maintain compatibility with the existing Ethernet/IP communication infrastructure.

4.2.6.3 Control Panels & Electrical Distribution

Control panels at the OPR Water Filtration Plant are distributed throughout the plant’s process areas, with PLCs installed in dedicated MCC sections and standalone enclosures. The plant’s control panels benefit from indoor installation, which reduces environmental exposure compared to the remote HQ System field sites. Electrical distribution follows plant-standard practices with panelboards and circuit breakers feeding individual control panel sections. The same general standards for electrical safety, including UL508A compliance, voltage separation, surge protection, and proper labeling, apply to the OPR plant infrastructure. Network connectivity at the plant is provided through Ethernet switches supporting the Ethernet/IP communication backbone, and any upgrades should incorporate managed switches to support cybersecurity monitoring and network segmentation in accordance with ISA 62443 standards.

4.2.7 PLC & Process Control

The PLCs that make up the process control system are distributed throughout various

areas of the plant and are dedicated to specific processes. A main PLC is configured with redundant CPUs in a hot/standby arrangement; notably, the primary and secondary PLC nodes are installed in separate buildings and are separated by a significantly greater distance than is typically encountered for redundant CPU configurations.

4.2.7.1 PLC Platform

The primary PLC platform is Allen Bradley ControlLogix.

4.2.7.2 Software Standards

The PLC standard is consistent with current integrator’s standard (South Coast Systems), but District does not have a documented standard reflecting the current system.

4.2.7.3 Process Control

The process control narratives for the PLCs are provided as Companion Document D.

4.3 SUMMARY REVIEW HIGHLIGHTS

4.3.1 Documentation Summary Review Highlights

The majority of documents collected consisted of scanned hard copies from remote sites, a limited set of drawings for the Headquarters (HQ) SCADA system, and contract drawings for the OPR SCADA system. Remote site documentation included design drawings, operations and maintenance manuals (O&Ms), and PLC program binders (“blue books”).

All documents were reviewed, analyzed, then consolidated in an organized manner. Generic materials – such as product specifications and manufacturer manuals – have been removed from the post-review deliverables to streamline the final document set. Both the original and consolidated files have been provided in digital format.

A consolidated Excel spreadsheet detailing remote site I/O and control relationships has been developed for District reference and issued as Companion Document A.

The consolidated blue books provided valuable insight into remote site configurations. With a few exceptions (e.g., the Arsenic Plant), most remote facilities fall into three primary categories: Wells, Booster Pump Stations, and Reservoirs. Within each category, I/O structures are generally consistent. This standardization presents a strong opportunity to streamline PLC modernization efforts by developing category-based templates and standards, improving efficiency, and reducing implementation complexity.

4.3.2 Configuration Summary Review Highlights

The District operates two fully independent SCADA systems – the Distribution System (HQ) at District Headquarters and the Water Filtration Facility System at the Oliver P. Roemer (OPR) Water Filtration Facility. The two systems use separate platforms, infrastructure, and operational workflows.

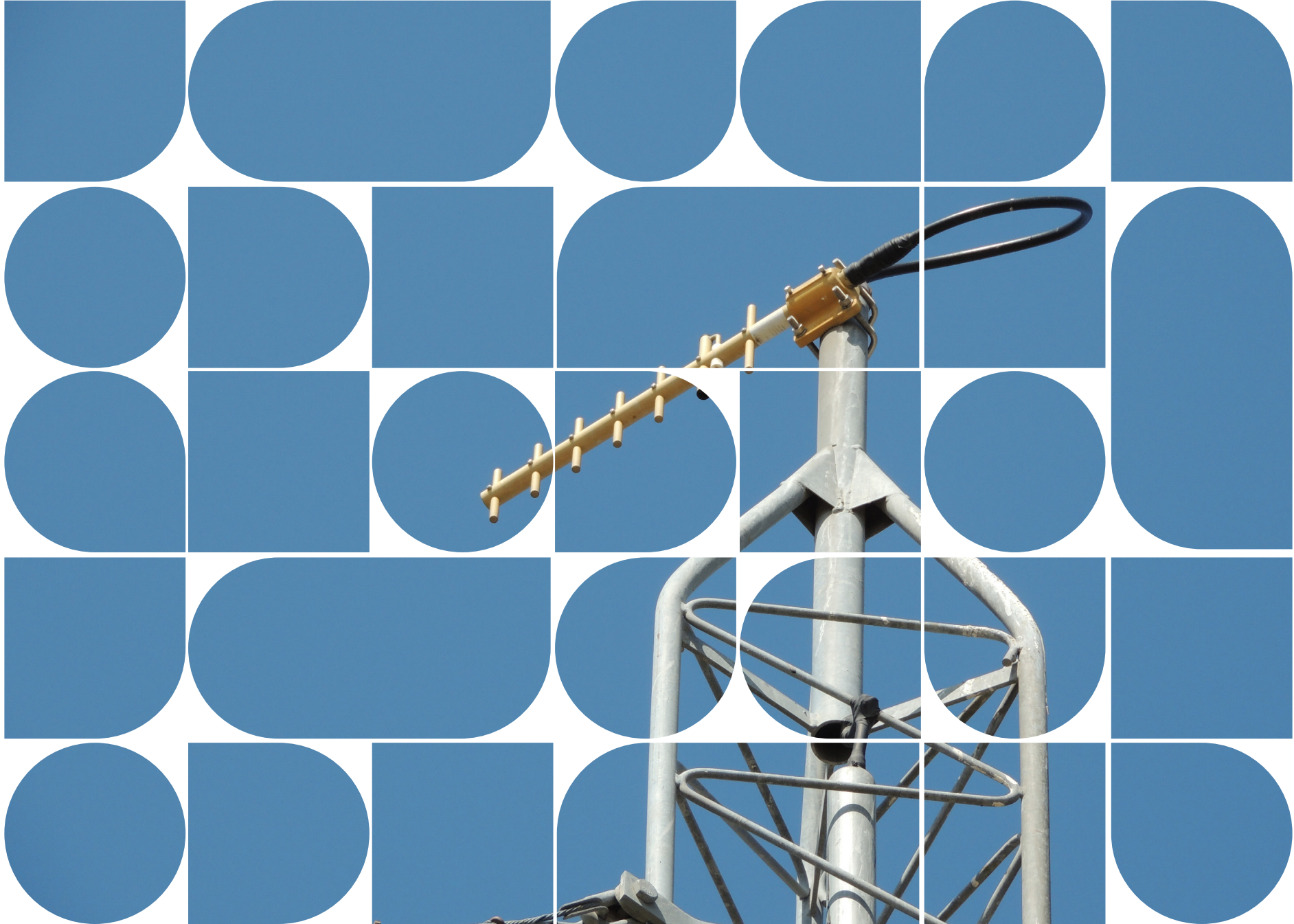
The HQ System runs on Wonderware InTouch with a Wonderware Historian, hosted on two standalone Dell PowerEdge hypervisors using a legacy version of VMware ESXi with no shared storage or automated failover. Despite the age of its computing and control components, the HQ System adheres to a moderately modernized cybersecurity architecture with structured ICS zone-based network segmentation utilizing Next Generation Firewall (NGFW) as the primary enforcement boundary. Remote sites are polled over a licensed 900 MHz serial radio network using proprietary Tesco Data Express protocols, and the PLC platform is predominantly legacy Tesco LIQ controllers serviced exclusively by Tesco Controls.

The OPR System runs on AVEVA System Platform with redundant I/O Servers and dual Tier 1 Historians, hosted on a Dell VRTX blade chassis with three hypervisors in a licensed VMware vSphere cluster providing shared storage and automatic failover. The PLC platform is Allen-Bradley ControlLogix communicating over a fiber-optic Ethernet/IP LAN. Comprehensive review of ICS configuration was not available since the system had not been officially turned over to the District at the time the SMP was developed.

Operating as two independent environments creates operational inefficiencies, increases the maintenance burden, and limits consistent implementation of cybersecurity controls, alarm management, and disaster recovery across the enterprise. Unifying both systems

under a common platform and standardized architecture would reduce complexity and improve long-term maintainability – a core objective of the recommendations in this SMP.





5 | NEEDS ASSESSMENT (NA) SUMMARY

Three workshops were conducted with the District to collaboratively develop a needs assessment matrix. These sessions identified key pain points and operational use cases that define the District’s requirements and inform recommendations for future system upgrades. The topics addressed during each workshop are summarized below.

5.1 NA WORKSHOPS

5.1.1 NA Workshop 1 – SCADA & Infrastructure

- › SCADA Platform Comparison
- › Graphic Standards
- › Alarming & Notification Strategy
- › Historical Data & Analysis Tools
- › Redundancy & High Availability Components
- › Core Hardware & Software Considerations
- › Response & Recovery
- › Mobility

5.1.2 NA Workshop 2 – IT Support & Infrastructure Standards

- › IT Support Roles
- › Configuration Standards
- › Equipment Standards
- › Network Segmentation Standards
- › Internal OT Resources
- › Consistency between OPR

and HQ Systems

- › Future Primary SCADA Location

5.1.3 NA Workshop 3 – Field & PLC

- › Operator Safety and Code Compliance: UL508A validation, AC voltage separation, voltage labeling, and grounding practices
- › Electrical Safety Improvements: Surge protection devices (SPDs), lightning arrestors per NFPA 70 Articles 810 and 820, and RFI filter maintenance
- › Security Monitoring Enhancements: Intrusion switches on control panels for SCADA-based door alarm monitoring
- › Field Enclosure Standards: Enclosure replacement, backboard upgrades to Unistrut, consolidation of multi-enclosure sites, and thermal management (fans and filters)
- › PLC Platform Assessment: Migration path for legacy Tesco LIQ IV, L2000, L3000, L1000G, and Modicon Momentum PLCs to modern platforms
- › Backup Power Standardization: Transition from UPS systems to 12VDC charger with battery configurations rated for outdoor environments
- › Network and Communications: Managed Ethernet switch deployment, legacy MDS 9710 radio replacements, and coaxial cable grounding
- › Cybersecurity Considerations: ISA 62443 compliance, managed switch requirements, and network segmentation at field sites
- › Maintenance Standards: Internal lighting, panel cleaning schedules, fan filter replacement, battery replacement

programs, and wire labeling requirements

- › Site-Specific Condition Assessment Results: Review of condition ratings (1–5 scale) across all sites for control panels, PLCs, radios, backup power, and network equipment

5.2 SUMMARY OF NEEDS

The Needs Assessment Matrix summarizes the items collected during the NA workshops and is included as Companion Document M of the SMP. These needs are categorized and expanded below to provide criteria for the subsequent gap analysis.

5.2.1 SCADA

5.2.1.1 Alarming

5.2.1.1.1 Root Cause Analysis and Alarm Strategy Improvements

Most sites currently generate AC and DC power fail alarms. During certain events, numerous alarms are triggered simultaneously, making it difficult to identify the true cause of the issue. To improve troubleshooting and root cause analysis, the District would like to expand the available diagnostic information related to PLC health, I/O module status, and other indicators that provide deeper insight into the field process infrastructure.

The District would also like to eliminate or significantly reduce the use of “common” alarms, as these tend to be ambiguous and do not clearly indicate what is actually failing within the system. Instead, alarms should

be more specific, actionable, and better aligned with identifying the primary fault.

Additionally, the District would like to implement alarm suppression or dependency logic where appropriate, so that secondary or consequential alarms do not obscure the primary cause of a system failure. The goal is for operators and maintenance staff to quickly identify the root issue rather than react to a flood of related alarms.

5.2.1.2 Data Analysis Tools

5.2.1.2.1 Historical Data and Analytics Considerations

Additional process and system information should be captured and stored to support analytics, reporting, and post-event troubleshooting. In the current system, many available tags are not configured for storage in the Historian, which limits the ability to perform meaningful post-analysis.

Future Historian sizing should account for a significantly expanded tag set, including process, PLC health, I/O status, and other diagnostic data. The long-term data strategy should include sufficient storage capacity and performance headroom to retain high-resolution data over appropriate time horizons, enabling more effective root cause analysis, reporting, and system optimization.

5.2.1.3 Data Integration

5.2.1.3.1 Historian Platform and Data

Integration Considerations

AVEVA continues to offer a SQL-based Historian platform, which is similar to the District’s existing Historian implementation. The choice of underlying database technology is an important factor in determining how easily additional data sources can be integrated with SCADA data in the future.

The District has identified Hach WIMS as a potential solution for managing manually collected and laboratory data. Since Hach WIMS supports SQL-based databases, maintaining a SQL-based Historian architecture may provide advantages in terms of data integration, interoperability, and long-term analytics capabilities.

5.2.1.3.2 State Reporting and Manual Data Integration

State regulatory reporting is currently performed using daily log sheets maintained in Microsoft Excel. The District uses XLReporter for SCADA-based reporting, and a portion of SCADA data is incorporated into state reports by exporting data from the Wonderware Historian into Excel via the XLReporter add-in.

At present, the process of combining SCADA data with manually collected data is largely manual and relies on Excel spreadsheets, which increases effort and introduces opportunities for errors and inconsistencies. The District is interested in solutions that enable SCADA data and manually collected data to be combined within a unified reporting or data

management platform to streamline state reporting and reduce manual data handling.

In addition, the District has identified the need to track user attribution for manually entered data to support nonrepudiation and audit requirements. The ability to capture who entered or modified manual data will be an important consideration in evaluating any proposed solutions.

5.2.1.4 Licensing

5.2.1.4.1 Subscription vs. Perpetual Considerations

AVEVA utilizes a subscription-based licensing model, which is acceptable to the District. While some platforms currently offer perpetual licensing options, there is a clear industry trend toward subscription-based software models. As a result, licensing approaches may change over time, even for platforms that presently offer perpetual licenses.

Future system planning should account for this trend and consider the long-term implications of licensing models, including cost predictability, scalability, and vendor support.

5.2.1.5 Manufacturer Support

5.2.1.5.1 Local Support and Platform Familiarity

Local SCADA manufacturer support is an important consideration for the District. Wonderware InTouch was originally selected based on the availability of strong local vendor

and integrator support and the District’s familiarity with the Wonderware platform.

These factors remain important considerations in evaluating current and future SCADA platform options.

5.2.1.5.2 Lab Analyzer Visibility and Packaged System Integration

Visibility of Apartis Lab Analyzer data provided by packaged system vendors is critical to District operations, particularly because the FBR treatment plant is not directly integrated into the SCADA system. At the FBR plant, Lab Analyzer readings are transferred into SCADA using LinkMaster.

When analyzer values exceed defined thresholds, the system can initiate an automatic plant shutdown. As a result, ensuring reliable data transfer, clear visibility, and appropriate alarming of Lab Analyzer data is essential.

The Lab Analyzer at the FBR treatment plant should be explicitly included in the access and integration plan for the new SCADA system to ensure operators have timely insight into analyzer status, data quality, and shutdown conditions.

5.2.1.6 Redundancy & HA

5.2.1.6.1 Historian Redundancy Considerations

The District would like to evaluate redundancy at the Historian level, as the current system relies on a single Historian instance. Given the

critical nature of the process and SCADA data stored in the Historian, incorporating redundancy or failover capabilities would enhance system reliability, ensure data availability, and support continuity of operations during hardware, software, or network failures.

Future planning should consider options such as mirrored databases, hot standby instances, or cloud-based replication to mitigate the risk of single points of failure.

5.2.1.7 Reliability

5.2.1.7.1 SCADA System Reliability Concerns

The District has expressed concerns regarding the reliability of the current SCADA system. Operators have observed intermittent system slowdowns, which can indicate impending failures. These performance issues reduce confidence in the system’s ability to consistently support operations and timely response to alarms or events.

Future system planning should prioritize robustness, predictable performance, and high availability to ensure reliable monitoring and control of critical processes.

5.2.1.8 Notification

5.2.1.8.1 Alarm Notification and SMS Communication

The District currently uses TopView for alarm notifications via SMS, which replaced the previous WIN-911 V7 system.

TopView has proven more reliable for the District compared to WIN-911.

Looking forward, alarm notification options will depend on the SCADA platform selected. Built-in notification tools generally provide more basic functionality, while third-party solutions offer richer features and greater flexibility. Discussion during planning leaned toward a preference for a stable, feature-rich third-party SMS solution.

The District is comfortable continuing with SMS-based notifications and does not require voice-based alerting. WIN-911 Mobile was identified for evaluation as a potential mobile alarm notification solution.

5.2.1.9 Staffing & Training

5.2.1.9.1 SCADA Software

The District has not yet undertaken SCADA application development, though there is interest in doing so. The ability for the District to be self-reliant in basic SCADA application development should be considered when selecting a SCADA platform, but it is not the primary factor. Training could support this capability regardless of the platform chosen.

5.2.1.9.2 System Flexibility and District Independence

The current system lacks flexibility and makes it difficult for the District to implement changes. The District experiences challenges accessing and modifying the system across multiple layers, including SCADA, networking,

and PLC programming, which limits the ability to respond quickly to operational needs.

The District would like to increase its level of independence in maintaining and modifying the system. Future solutions should emphasize improved accessibility, clearer system ownership, and reduced reliance on external resources for routine configuration changes, troubleshooting, and enhancements.

5.2.1.9.3 Dedicated OT Resource

The District is open to hiring a dedicated OT resource with broad integration skills and experience, given the size of the OT environment and the level of ongoing support required to maintain it effectively.

5.2.1.9.4 Response and Recovery Plan Integration

The District is open to incorporating the existing cybersecurity response plan into a comprehensive SCADA system response and recovery plan, ensuring it addresses broad infrastructure failure scenarios.

5.2.1.10 User Interface

5.2.1.10.1 Mobile Devices

Laptops are the primary SCADA interface used by District staff, with tablets (iPads) also in use, followed by local workstations. The District values the flexibility provided by tablets and is interested in expanding mobile access to smartphones, provided the SCADA application graphics are suitable for

smaller screens. Future SCADA applications should therefore consider support for a range of mobile devices and screen sizes.

The existing HQ system was not developed to prioritize use of SCADA on mobile devices like smartphones and tablets; however, the new Roemer application was developed for touch screen thin clients as well as mobile tablets. A similar consideration will be recommended for the new HQ system to ensure the SCADA application is designed for use on these touch-screen devices with smaller interfaces as well as on larger stationary devices with keyboards and mice like client workstations. The District is ok with operating the new HQ system from mobile clients as they move site to site as opposed to localized clients at the remote sites.

5.2.2 Infrastructure

5.2.2.1 Equipment Standards

The District would like to standardize on as many components as practical to reduce the wide variety of existing asset types, such as network switches, servers, and clients.

5.2.2.1.1 Core Software - Virtualization Platform and Licensing Considerations

The current system utilizes a VMware hypervisor platform, with which the District is familiar. Development of a new system based on VMware is acceptable and aligns with existing District experience and infrastructure.

Subscription-based licensing options will be evaluated to determine whether multi-year

agreements can help manage and predict costs over time. In addition, the recently deployed Roemer infrastructure is also built on a VMware hypervisor platform, further supporting compatibility and standardization across District systems.

5.2.2.1.2 CORE HARDWARE - COMPUTING AND STORAGE

The compute and storage at Roemer is a Dell blade/hyperconverged system (VRTX). The District is comfortable standardizing on this platform for the HQ system to simplify management, even though they were not directly involved in its initial selection. However, since the Roemer infrastructure may be approaching end of life by the time the HQ system is designed and integrated, the District is also open to other redundant server/storage solutions, such as Penguin (formerly Stratus).

5.2.2.2 Facility Location

5.2.2.2.1 SCADA Infrastructure Location and Redundancy Planning

Primary and secondary SCADA servers are currently located at Headquarters (HQ). With HQ planned for relocation within the next five years, the District is evaluating alternative locations for the future SCADA infrastructure.

The FBR facility is being considered as the primary location for the new SCADA infrastructure, given its suitability to host core systems and its position within the District’s network architecture. The OPR

facility is also being considered for redundant secondary components and/or as an Emergency Operations Center (EOC) to support system response and recovery planning.

At present, a 24 GHz wireless link exists between Roemer and HQ, and additional network paths may be available from OPR, HQ, and Roemer. However, because the high-speed backbone is currently distributed from HQ, FBR represents the strongest candidate location for the primary SCADA infrastructure moving forward.

5.2.2.3 Redundancy & HA

5.2.2.3.1 Redundancy Planning and “Split-Brain” Risk

Careful consideration of “split-brain” risk should be part of any design that distributes redundant resources across multiple locations. This applies to both hardware and software systems.

If both hot redundant resources—for example, primary and secondary SCADA servers—are co-located at the same site, there is an increased risk of simultaneous failure or network partitioning that could impact system availability. In such cases, incorporating a third location as a cold backup or disaster recovery site is desirable and should be included in the backup and recovery plan to ensure continuity of operations.

Redundancy planning should balance operational availability, recovery time

objectives, and risk mitigation for both planned and unplanned outages.

5.2.2.3.2 Core Hardware

The District wants to ensure redundancy in core hardware components, including the OT firewall, core switching, storage, and compute resources. Similar recommendations should apply to the new Roemer infrastructure.

Currently, Roemer has only a single OT firewall, creating a single point of failure in the primary traffic-shaping device that routes traffic between OT networks. The core switching at Roemer is configured as a Cisco stack; the District prefers an active-active high-availability (HA) switch configuration to allow maintenance activities, such as firmware upgrades, without taking both switches offline. This approach, known as zero-downtime maintenance, is a capability the District wants to implement for both the new HQ system and the Roemer system.

5.2.2.4 Monitoring & Notification

5.2.2.4.1 Failure Monitoring

The District expressed interest in improved monitoring and notification for SCADA infrastructure component failures. Currently, failures may go unnoticed until they impact other systems. Monitoring solutions that leverage common protocols, such as SNMP, should be considered.

5.2.3 Networking & Telemetry

5.2.3.1 Configuration Standards

5.2.3.1.1 Network & Telemetry Traffic Architecture

The District would like to standardize certain configurations, such as implementing traffic-shaping policies primarily in the OT firewall rather than in core switching or other routing devices. With District replacing the existing Level 3 router used for internal segmentation with a Next-Generation Firewall (NGFW) to enhance ICS security architecture and align with Zero Trust principles. While the current router provides basic Access Control Lists (ACLs) for network segmentation, it lacks advanced security capabilities such as stateful inspection, deep packet inspection (DPI), application-layer awareness, intrusion detection and prevention (IDS/IPS), identity-based access control, and comprehensive security event logging. The NGFW will serve as an internal enforcement point between defined security zones, implementing zone-based policy enforcement, least-privilege communication matrices, and micro-segmentation controls to restrict east-west traffic and eliminate implicit trust based solely on network location. Additional capabilities including threat intelligence integration, anomaly detection, and centralized log forwarding will improve monitoring, audit defensibility, and incident response readiness. This architecture strengthens zone and conduit enforcement consistent with reduces lateral movement risk, and advances the District’s transition toward

a policy-driven, continuously monitored, and resilient Zero Trust-aligned ICS architecture.

This architecture will also implement Quality of Service (QoS) policies to ensure operational reliability by prioritizing critical ICS communications. SCADA telemetry traffic will be classified as high-priority, latency-sensitive traffic, ensuring guaranteed bandwidth and minimal delay across internal network segments. Secondary services such as network monitoring and data synchronization processes (e.g., historian replication or backups), which can tolerate buffering or minor delay, will be assigned lower priority or rate-limited queues. This QoS enforcement supports deterministic performance of operational systems while maintaining visibility and supporting services without allowing non-critical traffic to impact real-time control communications.

5.2.3.1.2 Network Segmentation

The existing Headquarters (HQ) and Roemer (OPR) systems currently implement differing approaches to network segmentation. The HQ system, although supporting a smaller asset footprint, employs more clearly defined network segments and separation controls. Conversely, the Roemer (OPR) system supports a significantly larger and more diverse operational asset base but lacks clearly defined and consistently enforced segmentation boundaries. This architectural inconsistency introduces increased risk of lateral movement, complicates policy

enforcement, and reduces visibility across the operational technology (OT) environments.

To address this risk and align with modern cybersecurity principles, the District will incorporate micro-segmentation controls within and between defined security zones to support Zero Trust Architecture (ZTA) principles. Micro-segmentation will restrict east-west communications based on explicit, policy-driven allowlists rather than broad network trust assumptions. By enforcing granular, identity- and service-based access controls at internal enforcement points, the District will eliminate implicit trust within the operational network and ensure that all system-to-system communications are explicitly authorized, continuously monitored, and limited to operational necessity. This approach strengthens containment capabilities, limits lateral movement in the event of compromise, and advances the District's transition toward a resilient, Zero Trust-aligned ICS architecture.

The District intends to establish a standardized, repeatable network segmentation framework that can be implemented for the new HQ system and retroactively applied to the Roemer (OPR) system. This unified segmentation model will align with the Purdue Enterprise Reference Architecture (PERA), ISA/IEC 62443 zone and conduit principles, and NIST SP 800-82r3 guidance. The objective is to achieve consistent architectural controls across both environments, enforce least-privilege communication between zones, improve

monitoring and logging visibility, and reduce the blast radius of potential cyber incidents while maintaining operational reliability.

5.2.3.2 Reliability

5.2.3.2.1 Radio Telemetry Backup Solution

The District has expressed interest in implementing Ethernet radios with a cellular backup option to provide communication redundancy for remote sites within the HQ system. This approach would help ensure continued operation in the event of RF disruptions, such as antenna or cable vandalism, particularly where components are exposed.

At a minimum, critical sites - and potentially Access Points (which hosts number of remotes) - should be evaluated for cellular backup capability. The District is open to forward-looking strategies, including specifying radio hardware that supports integrated cellular redundancy, to strengthen the overall reliability of remote communications.

This approach would also provide greater flexibility for potential secondary SCADA or Emergency Operations Center (EOC) sites by reducing reliance on radio communications from a single originating location, as is currently the case with HQ.

5.2.3.3 Resource Considerations

5.2.3.3.1 Communication Bandwidth Between Redundant Components

AVEVA and VT SCADA platforms require significantly higher bandwidth between redundant components to maintain proper synchronization and performance. This becomes a critical design consideration when primary and secondary SCADA servers are deployed at separate facilities interconnected through a site-to-site communication link.

In accordance with manufacturer recommendations and to ensure optimal reliability, both redundant SCADA servers should be co-located within the same facility, where a stable and dedicated 1 Gbps connection can be provided specifically for redundancy traffic. This approach minimizes latency, reduces synchronization risk, and ensures consistent system performance during failover events.

5.2.4 Field

5.2.4.1 Enclosures & Environmental Controls

5.2.4.1.1 Field Enclosure Conditions and Retrofit Considerations

The needs assessment workshop reviewed the condition and sizing of field enclosures across District remote sites. Most motor control centers (MCCs) are approximately 70 inches high by 22 inches wide, while smaller remote terminal unit (RTU) panels are approximately 28 inches high by 22 inches wide. The assessment found that many MCCs are in serviceable condition and are candidates for retrofitting with updated control components rather than full replacement. However, some smaller en-

closures and older panels exhibit rust, deteriorated backboards, and structural degradation that necessitates full enclosure replacement. Backboards at such sites should be upgraded to Unistrut-based configurations to improve modularity and support future equipment changes.

Proper environmental controls are critical for reliable electronics operation in outdoor installations. The District identified a need to equip outdoor panels with cooling fans or air conditioners to manage internal temperatures. The use of panel heaters is not recommended, as heaters can contribute to component stress and increased maintenance burden over time. Heaters should only be installed if where documented condensation cannot be controlled by ventilation or enclosure selection. Where multiple enclosures exist at a single site, consolidation into a single enclosure should be evaluated to reduce complexity and simplify ongoing maintenance.

5.2.4.1.2 Backup Power Considerations

For backup power in high-temperature outdoor environments, battery-based backup systems are preferred over uninterruptible power supply (UPS) units. UPS equipment is generally less reliable under sustained high ambient temperatures. Battery backup systems using 12 VDC charger and battery configurations are better suited to the District's field conditions. A regular battery replacement program on a three- to five-year cycle is recommended to maintain reliability and prevent unplanned outages due to battery degradation.

5.2.4.2 Asset Condition Assessment

5.2.4.2.1 Condition Ranking and Prioritization

A five-level ranking system was introduced during the workshop to categorize field asset conditions from excellent to critical. This framework enables the District to systematically prioritize maintenance activities and capital upgrades based on objective condition criteria. Site-specific condition assessment results, covering control panels, PLCs, radios, backup power systems, and network equipment, have been documented in the Companion Document that will be made available for District review, enabling informed and targeted investment decisions across the field asset portfolio.

Common deficiencies identified across field sites include inconsistent or missing wire and terminal labeling, absence of intrusion switches on control panel doors, and non-uniform grounding practices. These deficiencies increase troubleshooting time and reduce the reliability of fault isolation. The District requires standardized labeling of all field wiring and instrumentation connections, and the installation of intrusion switches on control enclosures to enable SCADA-based door alarm monitoring as part of the broader security enhancement effort.

5.2.4.3 Communications & Cybersecurity

5.2.4.3.1 Network Switch and Radio Modernization

Obsolete communication equipment at remote field sites presents both operational reliability and cybersecurity risks. The District identified the need to replace legacy radios and unmanaged network switches with managed Ethernet switches and modern radio hardware. Managed switches provide essential cybersecurity capabilities—including VLAN segmentation, port-level access control, and event logging—that are not available on unmanaged devices. This transition is necessary to align field site communications infrastructure with ISA/IEC 62443 security principles and to support consistent network visibility across all District sites.

5.2.4.4 Maintenance Standards

5.2.4.4.1 Ongoing Maintenance Requirements

The workshop emphasized the importance of establishing and enforcing consistent field maintenance standards across all remote sites. Recommended practices identified during the needs assessment include regular cleaning of cooling fan filters to prevent thermal management failures, proper labeling and re-labeling of field wires following any modifications, and the installation of internal panel lighting to facilitate safe and efficient troubleshooting in the field. Adherence to these standards is intended to reduce corrective maintenance burden and support District staff in performing routine inspections and repairs efficiently and safely.

5.2.5 PLC

5.2.5.1 Platform Evaluation & Selection

5.2.5.1.1 Allen-Bradley vs. Schneider Electric Platform Comparison

The needs assessment workshop evaluated two PLC platforms for use in the District’s distributed remote site control systems: the Schneider Electric M340 and the Allen-Bradley CompactLogix. Both platforms support hot-swappable hardware modules and SD card-based configuration and firmware backups, and both are appropriate for deployment in remote site environments. The workshop concluded that the Allen-Bradley CompactLogix is the preferred platform for the District, primarily due to existing familiarity among District staff and integrators, and the opportunity to standardize the remote site PLC environment with the OPR Water Filtration Plant, which already utilizes Rockwell Automation equipment.

The Schneider Electric M340 offers native Modbus RTU and Modbus TCP support, which simplifies integration with legacy Tesco PLCs currently installed at District remote sites. Due to limited bandwidth of RF communication, additional configuration consideration is needed as Allen-Bradley native protocol cannot be utilized. Despite this additional integration consideration, the District determined that the long-term operational and training benefits of a standardized Allen-Bradley platform outweigh the initial cost and configuration overhead. Upgrade projects should be sequenced and grouped in

logical site clusters to minimize operational disruptions during the transition period.

5.2.5.1.2 Cybersecurity and Platform Security Considerations

Both the Allen-Bradley CompactLogix and the Schneider Electric M340 platforms comply with ISA/IEC 62443 industrial cybersecurity standards. Each platform provides password-protected access controls, firmware signing to prevent unauthorized firmware modifications, and built-in diagnostic tools that support monitoring and troubleshooting activities. These security capabilities are baseline prerequisites for any PLC platform selected for the District’s modernized remote site control infrastructure.

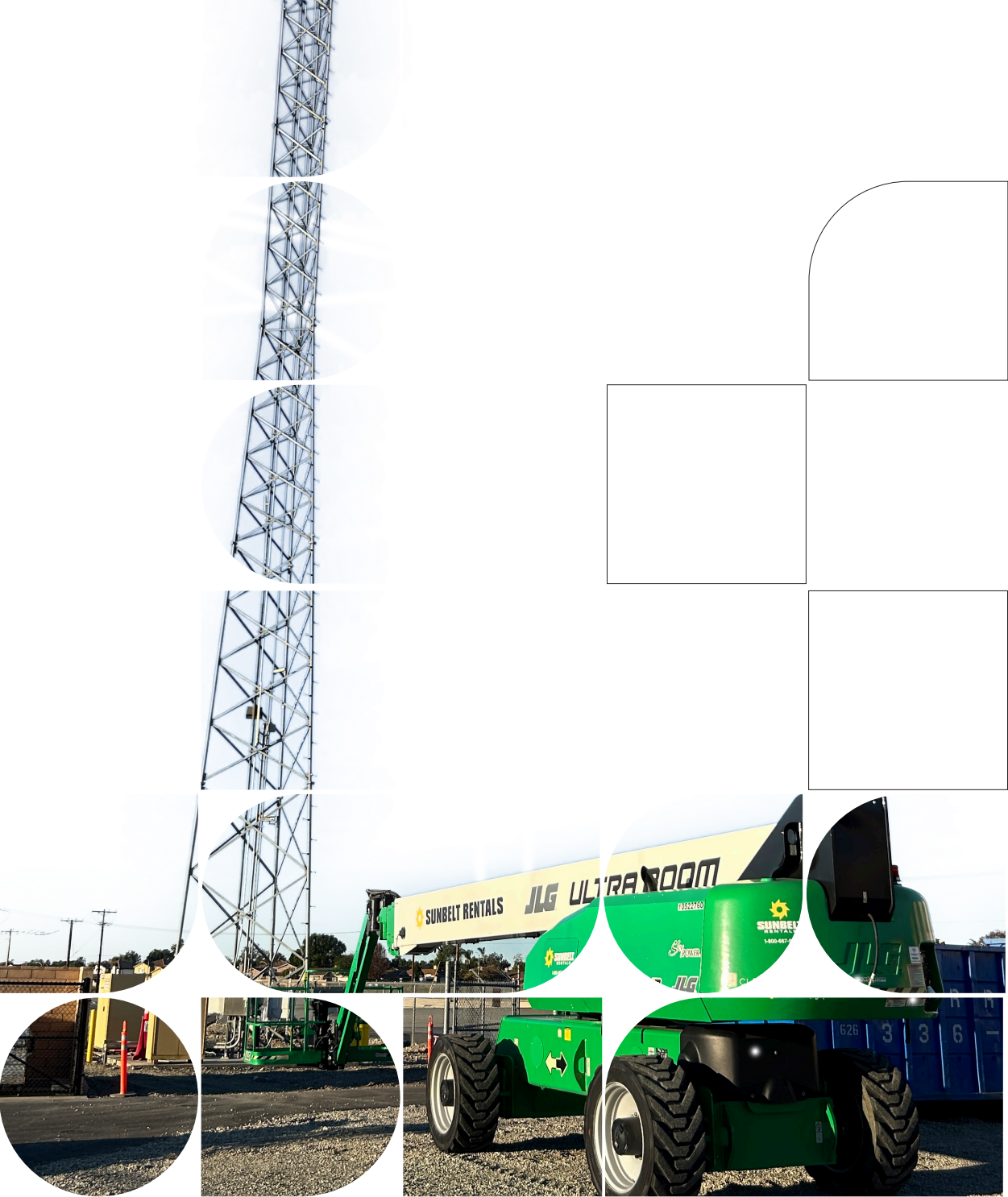
5.2.5.2 Programming Standards

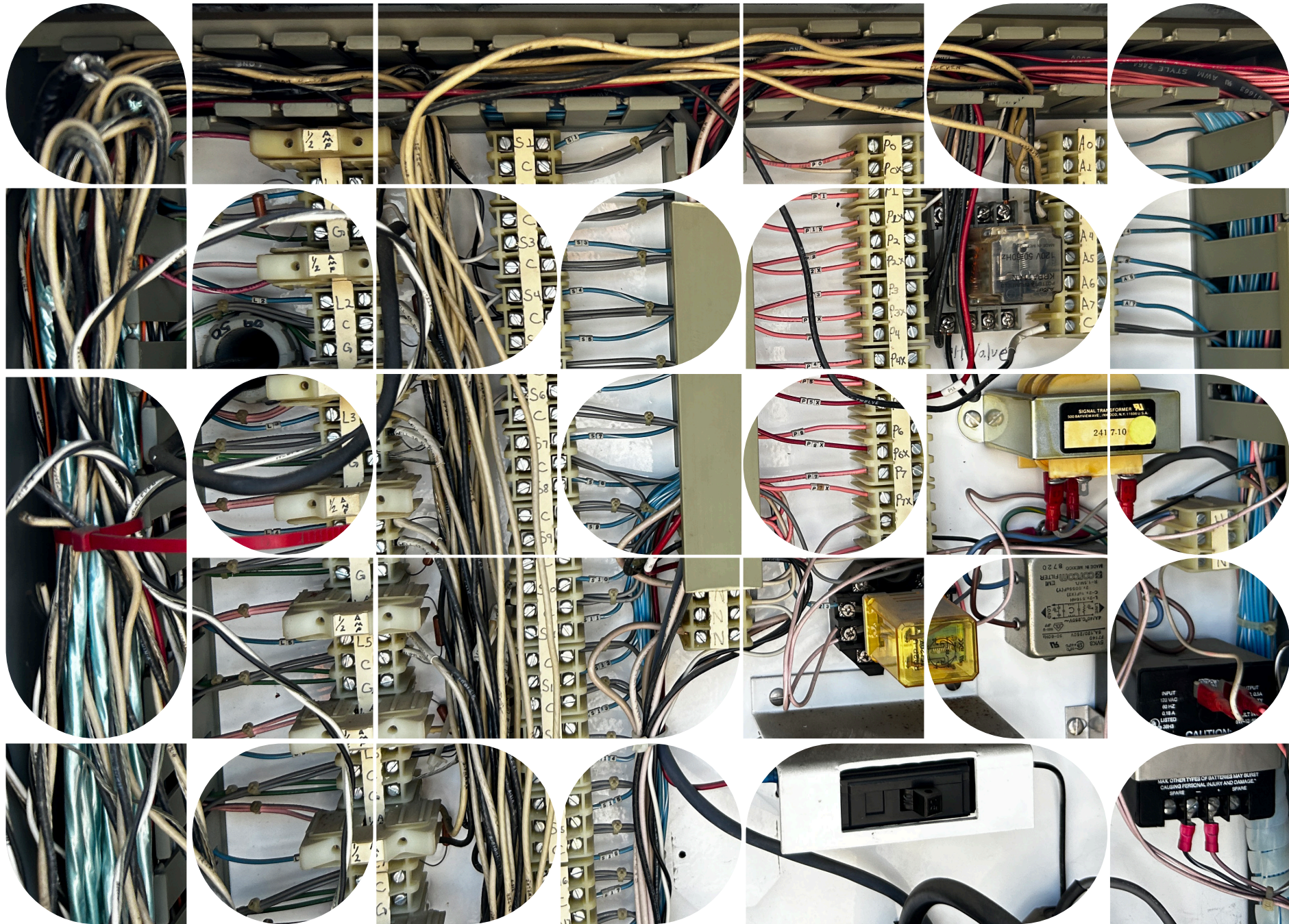
5.2.5.2.1 Code Structure, Tag Naming, and Documentation Requirements

Standardizing PLC programming practices was identified as a critical requirement to support long-term maintainability, simplified troubleshooting, and effective knowledge transfer among District staff and integrators. The District has established some programming standards through previous projects; however, consistent enforcement and comprehensive documentation of those standards remain areas requiring improvement.

Key elements of the PLC programming standard include consistent and descriptive tag naming conventions, a well-organized code structure with clear task separation,

and thoroughly documented process control narratives that describe the intended behavior of each control sequence. Both evaluated PLC platforms integrate with major SCADA systems, including AVEVA System Platform, enabling a standardized approach to tag mapping and data exchange between the field control layer and the SCADA application layer. Establishing and enforcing these programming standards across all future PLC projects will ensure that the District’s control systems remain supportable, auditable, and adaptable as operational requirements evolve.





6 | CYBERSECURITY EVALUATION

6.1 SECURITY CONTROLS GAP ASSESSMENT

A security controls gap assessment was conducted to determine the District's current cybersecurity maturity level. The assessment was based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and evaluated both the District's cybersecurity policies and operational practices. The results of this assessment were used to develop a baseline Cybersecurity Policy, a Cybersecurity Requirements Specification (CRS), and a draft Incident Response and Recovery Plan for the District.

The full cybersecurity assessment report was provided to the District as a separate document. A summary of the assessment is provided in the sections below that includes the maturity level results and the significant findings organized by NIST CSF function and category.

6.2 ASSESSMENT SUMMARY

6.2.1 Maturity Level Descriptions

The framework uses a maturity model to score the security controls against a target level. Policy maturity is a measurement of how well the organization's policies, procedures, standards, and guidelines satisfy the framework requirements. Process maturity is a measurement of how well the organization's actual

operational practices satisfy the framework requirements, regardless of what the policies

and standards indicate or even whether policies or standards are formally defined.

FIGURE 1 CYBERSECURITY MATURITY LEVEL EXPECTATIONS

Maturity Level	Level Description	Maturity Level Expectations
0	Not Implemented	Policies do not exist or processes are not performed.
1	Initial	A policy or process is partially implemented or performed but is ad-hoc or reactive.
2	Repeatable	A policy or process exists but may have gaps. Protection mechanisms and monitoring are implemented, and basic to moderate analysis and performance measurements take place.
3	Defined	Organization-wide policy or process exists with formal management approval and is consistently adhered to. Evidence can be provided for most activities. Projects are planned, performed, measured, and controlled.
4	Managed	Organization is data-driven with quantitative performance improvement objectives aligned to meet internal and external stakeholder needs. Continuous monitoring is implemented ubiquitously and response and recovery time and impact monitored and minimized.
5	Optimizing	Organization is focused on continuous improvement and capable of pivoting and responding to opportunity and change. Standardized and optimized processes are implemented and improvement information is shared and communicated throughout the organization.
2	Target Level	

Security controls are requirements that are used as a baseline metric to evaluate systems

CSF 2.0 controls organized into 22 categories and distributed into six framework functions.

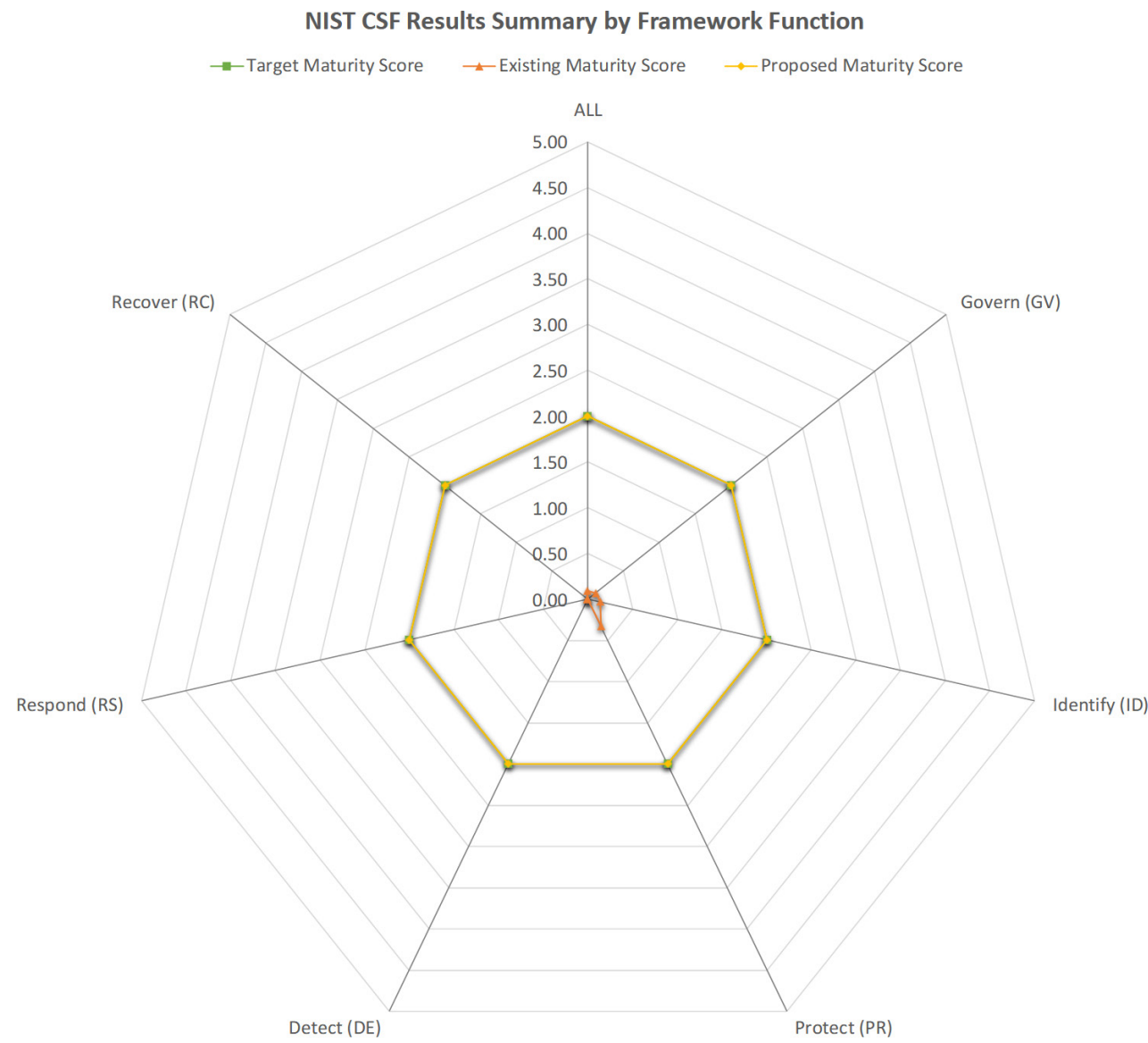
Framework Function Heat Map Table

Function	Control Category	Target	Existing	Proposed
Govern	Category Totals (/31) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.11	2.00
Identify	Category Totals (/21) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.14	2.00
Protect	Category Totals (/22) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.33	2.00
Detect	Category Totals (/11) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.00	2.00
Respond	Category Totals (/13) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.00	2.00
Recover	Category Totals (/8) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2.00	0.00	2.00

Function	Control Category	Target	Existing	Proposed
Govern	(GV. OC) Organizational Context	2.00	0.30	2.00
Govern	(GV. RM) Risk Management Strategy	2.00	0.00	2.00
Govern	(GV. RR) Roles, Responsibilities, and Authorities	2.00	0.25	2.00
Govern	(GV. PO) Policy	2.00	0.00	2.00
Govern	(GV. OV) Oversight	2.00	0.00	2.00
Govern	(GV. SC) Cybersecurity Supply Chain Risk Management	2.00	0.10	2.00
Identify	(ID. AM) Asset Management	2.00	0.14	2.00
Identify	(ID. RA) Risk Assessment	2.00	0.15	2.00
Identify	(ID. IM) Improvement	2.00	0.13	2.00
Protect	(PR. AA) Identity Management, Authentication, and Access Control	2.00	0.42	2.00
Protect	(PR. AT) Awareness and Training	2.00	0.00	2.00
Protect	(PR. DS) Data Security	2.00	0.38	2.00
Protect	(PR. PS) Platform Security	2.00	0.33	2.00
Protect	(PR. IR) Technology Infrastructure Resilience	2.00	0.50	2.00
Detect	(DE. CM) Continuous Monitoring	2.00	0.00	2.00
Detect	(DE. AE) Adverse Event Analysis	2.00	0.00	2.00
Respond	(RS. MA) Incident Management	2.00	0.00	2.00
Respond	(RS. AN) Incident Analysis	2.00	0.00	2.00
Respond	(RS. CO) Incident Response Reporting and Communication	2.00	0.00	2.00
Respond	(RS. MI) Incident Mitigation	2.00	0.00	2.00
Recover	(RC. RP) Recovery Planning	2.00	0.00	2.00
Recover	(RC. CO) Communications	2.00	0.00	2.00

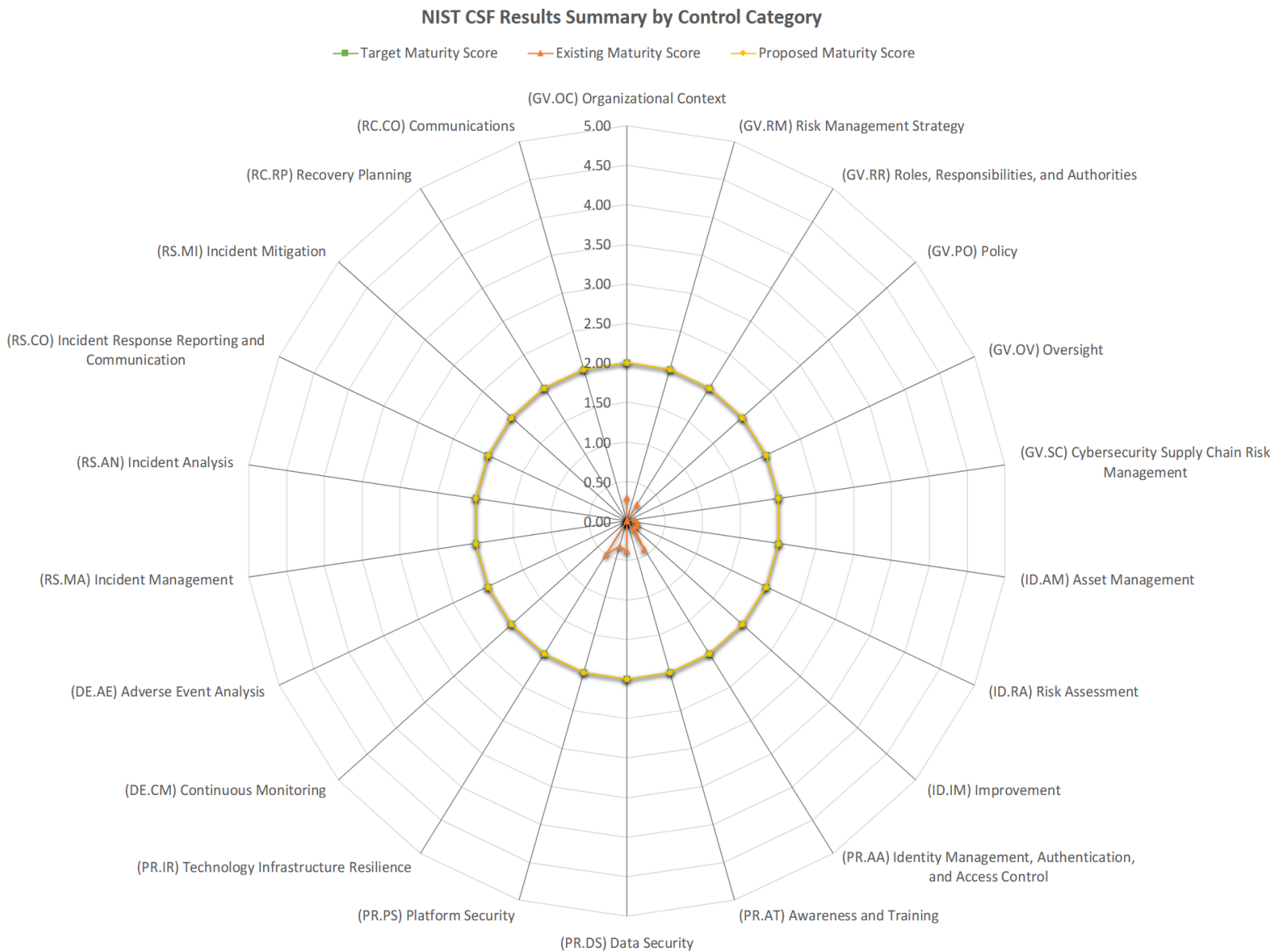
6.2.3 Maturity Level Results by Function

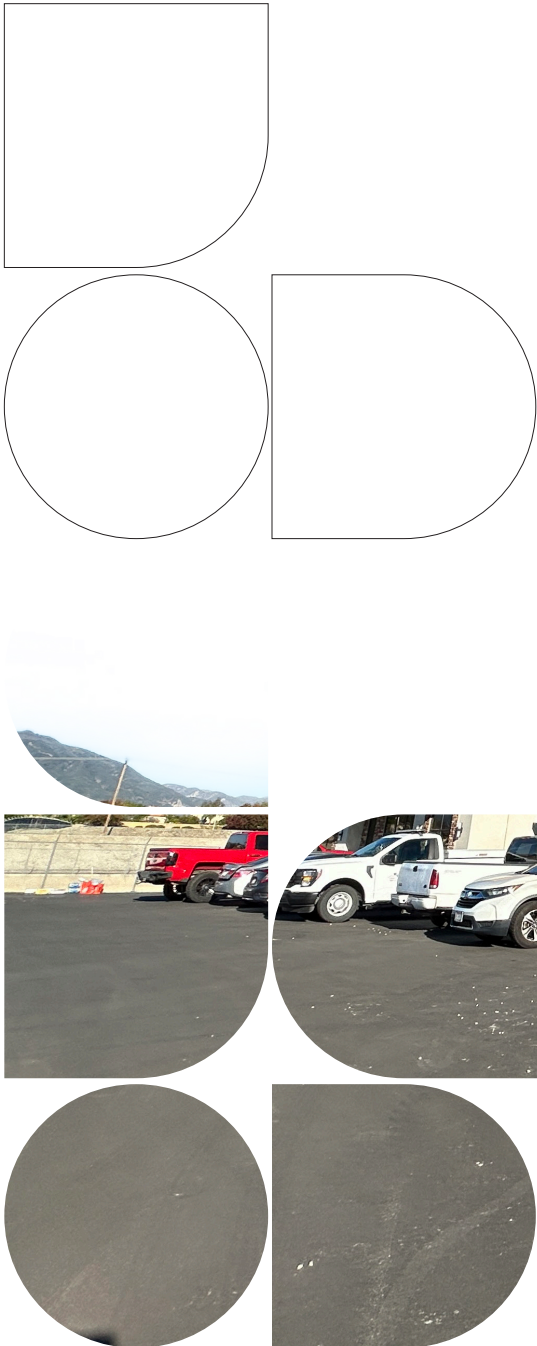
FIGURE 3 CYBERSECURITY MATURITY LEVEL RESULTS BY FUNCTION DIAGRAM



6.2.4 Maturity Level Results by Category

FIGURE 4 CYBERSECURITY MATURITY LEVEL RESULTS BY CATEGORY DIAGRAM





6.3 ASSESSMENT FINDINGS

A follow-on Cybersecurity Controls Reassessment Project has been identified in the project recommendations section of this SMP. The objective of this effort is to reassess and update the District’s cybersecurity

maturity level following the implementation of the baseline Cybersecurity Policy and the Incident Response and Recovery Plan. Because these initiatives significantly influence maturity scoring, their implementation is expected to materially improve the District’s cybersecurity maturity baseline.

6.3.1 Security Control Functions

FIGURE 5 SECURITY CONTROL FUNCTION DESCRIPTIONS TABLE

Function	Focus	Description
Govern (GV)	The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization’s broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
Identify (ID)	The organization’s current cybersecurity risks are understood.	Understanding the organization’s assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization’s policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions
Protect (PR)	Safeguards to manage the organization’s cybersecurity risks are used.	Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
Detect (DE)	Possible cybersecurity attacks and compromises are found and analyzed.	DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
Respond (RS)	Actions regarding a detected cybersecurity incident are taken.	RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
Recover (RC)	Assets and operations affected by a cybersecurity incident are restored.	RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

6.3.2 Governance Summary

6.3.2.1 Operational Context

Risk management is currently an informal process, and no formal procedures have been defined. The District’s critical services and capabilities are recognized and generally understood; however, they have not been formally documented or addressed organization-wide through a top-down governance approach. This formalization will be partially achieved through the completion and implementation of the in-progress Cybersecurity Policy developed for the District. External dependencies that represent potential points of failure for the District’s critical capabilities and services are generally understood by appropriate personnel but are not formally documented. The District does not currently have an official Non-Disclosure Agreement (NDA) or a formal process for implementing one; however, a Cybersecurity Requirements Specification (CRS) is currently in development.

6.3.2.2 Risk Management Strategy

The District does not have a formal risk management strategy in place to capture and communicate priorities or constraints that would inform organizational risk tolerance and risk appetite. There is no documented guidance to support decision-making related to cybersecurity risk across the organization. Users currently have no formal process or guidance for surfacing cybersecurity-related questions or concerns. Additionally, there is no standardized method for identifying,

calculating, documenting, categorizing, or prioritizing cybersecurity risks.

6.3.2.3 Roles, Responsibilities, and Authorities

No specific cybersecurity or risk management roles have been formally defined for the District. There is no designated Chief Information Security Officer (CISO), nor is there an individual formally assigned responsibility for cybersecurity oversight across the organization. Job descriptions generally do not define cybersecurity-related responsibilities for users. There is no dedicated or independent budget allocated for Operational Technology (OT) cybersecurity. Furthermore, there is no formalized onboarding or termination process, and no documented procedure exists for removing or revoking credentials on the OT side.

6.3.2.4 Policy

No formal vulnerability assessment policy or process exists. A formal risk assessment program has not been established to identify and document risk components as part of a structured assessment process. Additionally, no formal risk assessment process exists to determine specific cybersecurity risks or to support the development of appropriate risk response strategies. Senior management is not directly involved in the development, approval, oversight, or management of cybersecurity policies.

6.3.2.5 Oversight

No formal risk management strategy or framework has been established, and no processes exist to capture, communicate, or enforce organizational risk tolerance. While the District is aware of its role in delivering critical services, it has not established a formal risk management framework or defined an informed risk tolerance aligned with its responsibilities as a critical service provider.

6.3.2.6 Supply Chain Risk Management

No formal supply chain risk management program has been established for cyber-related components and services. The District has not defined appropriate service-level agreements (SLAs), identified or tracked supplier-related threats and vulnerabilities, established protocols for information sharing, or defined cybersecurity requirements based on supplier criticality and potential impact. Additionally, there are no formal requirements for incident response and recovery reporting by suppliers, nor are suppliers required to provide evidence of compliance with the District’s cybersecurity expectations.

6.3.3 Identification Summary

6.3.3.1 Asset Management

No tools are currently in place to manage hardware and software assets on the OT side. While OT asset inventory efforts are being partially addressed through ongoing projects, a more formalized and repeatable asset management process is required. Asset

refresh cycles are not formally documented and are not consistently followed.

6.3.3.2 Risk Assessment

No formal vulnerability assessment or risk assessment process has been established. A structured risk assessment program that would enable risk components to be identified, analyzed, and documented has not been implemented. As a result, the District does not have a formalized process to identify specific cybersecurity risks or to develop and document appropriate risk response strategies.

6.3.3.3 Improvements

There are currently no formalized cybersecurity policies or procedures in place. However, the District is in the process of developing a comprehensive Cybersecurity Policy, along with a Cybersecurity Requirements Specification (CRS) and Incident Response and Disaster Recovery plans. Follow-up initiatives will be defined within a Master Plan to support the implementation of these efforts, as well as to identify recommended projects for additional cybersecurity improvements.

6.3.4 Protection Summary

6.3.4.1 Identity Management, Authentication, and Access Control

Informal processes are in place to manage local and remote access, including the use of multi-factor authentication (MFA). However, the management of user identities

and credentials is not formalized through documented policies or procedures.

6.3.4.2 Awareness and Training

Some level of cybersecurity awareness exists among individual employees; however, no formalized cybersecurity awareness or training program is in place. Cybersecurity-specific responsibilities are not defined within job roles or position descriptions.

6.3.4.3 Data Security

No formalized policies or procedures have been established to ensure consistent and effective data protection practices across the organization.

6.3.4.4 Platform Security

No configuration management solution has been implemented OT environments. Additionally, no formalized policies or procedures exist to address unsupported or end-of-life software and hardware throughout the asset lifecycle. There are also no documented procedures for performing system audits or for implementing non-repudiation controls.

6.3.4.5 Technology Infrastructure Resilience

Some logical network segmentation has been implemented; however, there are no formalized policies or procedures to guide the design, implementation, or ongoing management of resilient infrastructure architectures.

6.3.5 Detection Summary

6.3.5.1 Continuous Monitoring

In the Continuous Monitoring category, no Security Information and Event Management (SIEM) or comparable monitoring solution has been implemented. Additionally, there are no formalized policies or procedures in place to support continuous monitoring activities.

6.3.5.2 Adverse Event Analysis

No centralized logging or auditing infrastructure exists to support real-time detection, analysis, or investigation of adverse cybersecurity events. Furthermore, no formalized policies or procedures have been established to guide the implementation or operation of adverse event analysis capabilities.

6.3.6 Response Summary

6.3.6.1 Incident Management

No formal incident response plan has been established.

6.3.6.2 Incident Analysis

Incident investigations are conducted on a case-by-case basis due to the absence of a formalized incident response plan and defined analysis procedures.

6.3.6.3 Incident Response Reporting and Communications

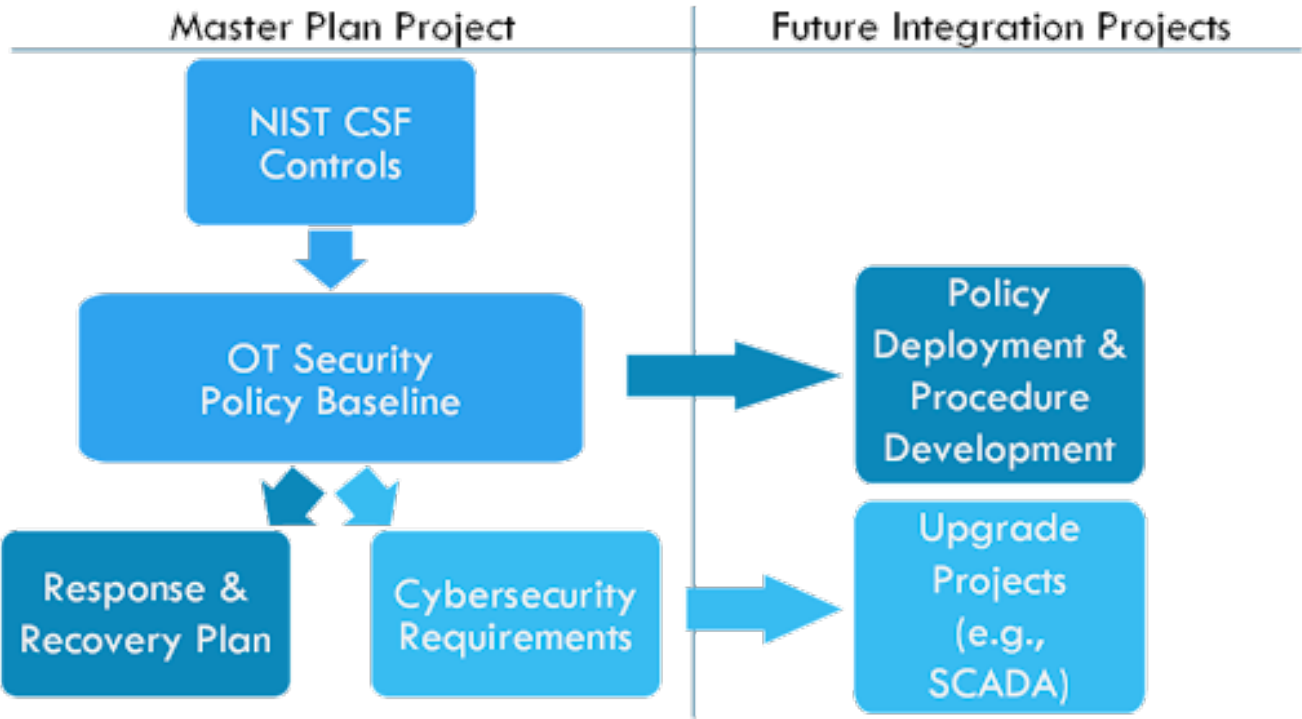
No formal incident response plan exists to guide internal or external reporting, escalation, or communication activities. 6.3.6.4 Incident Mitigation No formal incident response plan has been established. Mitigation actions are handled on a case-by-case basis without documented procedures or defined roles. 6.3.7 Recovery Summary 6.3.7.1 Incident Recovery Plan Execution	No formal incident recovery plan has been established to guide recovery activities following a cybersecurity incident. 6.3.7.2 Incident Recovery Communications No formal recovery plan exists to guide internal or external communications during or following recovery activities. 6.4 BASELINE SECURITY POLICY A baseline security policy was created for the District as a component of the SCADA Master Plan encompassing the development of cybersecurity policies, which is now owned	and overseen by the District. The baseline policy was refined through collaborative workshops to tailor individual aspects to the District and consists of multiple individual policies, each addressing specific focus areas, and structured as a comprehensive security policy for the District's OT. Individual policies in the resulting baseline security policy were derived from NIST CSF controls and then tailored to meet specific needs of the District. The Cybersecurity Requirements Specification (CRS) was then developed from relevant policy items. This relationship is represented in the following diagram.
--	---	--

FIGURE 6 SECURITY CONTROLS, POLICY, REQUIREMENTS RELATIONSHIP DIAGRAM



The baseline security policy sets guidelines for protecting the District's OT, which encompasses the data and assets associated with the water process control systems, as well as the personnel responsible for their operation and maintenance, against security threats. It defines the methods for safeguarding the assets and data that comprise the District's OT Systems,	ensuring that all individuals comprehend their responsibilities and the appropriate actions to take for secure operations, thereby establishing a framework for sustaining a secure environment and reducing risks to this essential infrastructure. The baseline security policy was provided to the District as a separate document. The integration effort of this baseline	policy has been defined in the project recommendations section of this SMP. The baseline security controls, baseline policy, response and recovery plan, and cybersecurity requirements developed as part of the SMP project and their relationship to future integration projects is represented in the following diagram.
---	---	--

FIGURE 7 MASTER PLAN PROJECT AND FUTURE INTEGRATION PROJECTS RELATIONSHIP DIAGRAM



6.5 CYBERSECURITY REQUIREMENTS SPECIFICATION (CRS)

A cybersecurity requirements specification (CRS) was developed to define the requirements that comprise the District’s OT security policy. The requirements were extracted from the baseline security policy to ensure alignment between the requirements themselves and the policy enforcing them. The requirements defined in the CRS are essential guidelines that must be adhered to for all project work (moving forward) that involves District OT systems by internal District staff and outside third parties. This CRS will be distributed to the appropriate 3rd parties performing design, engineering, and integration projects within the OT environment to ensure the District’s Cybersecurity requirements are included for all relevant projects from their inception through completion. The CRS was provided to the District as a separate document and is referenced by several project recommendations, as well as the system design criteria related to Cybersecurity standards.

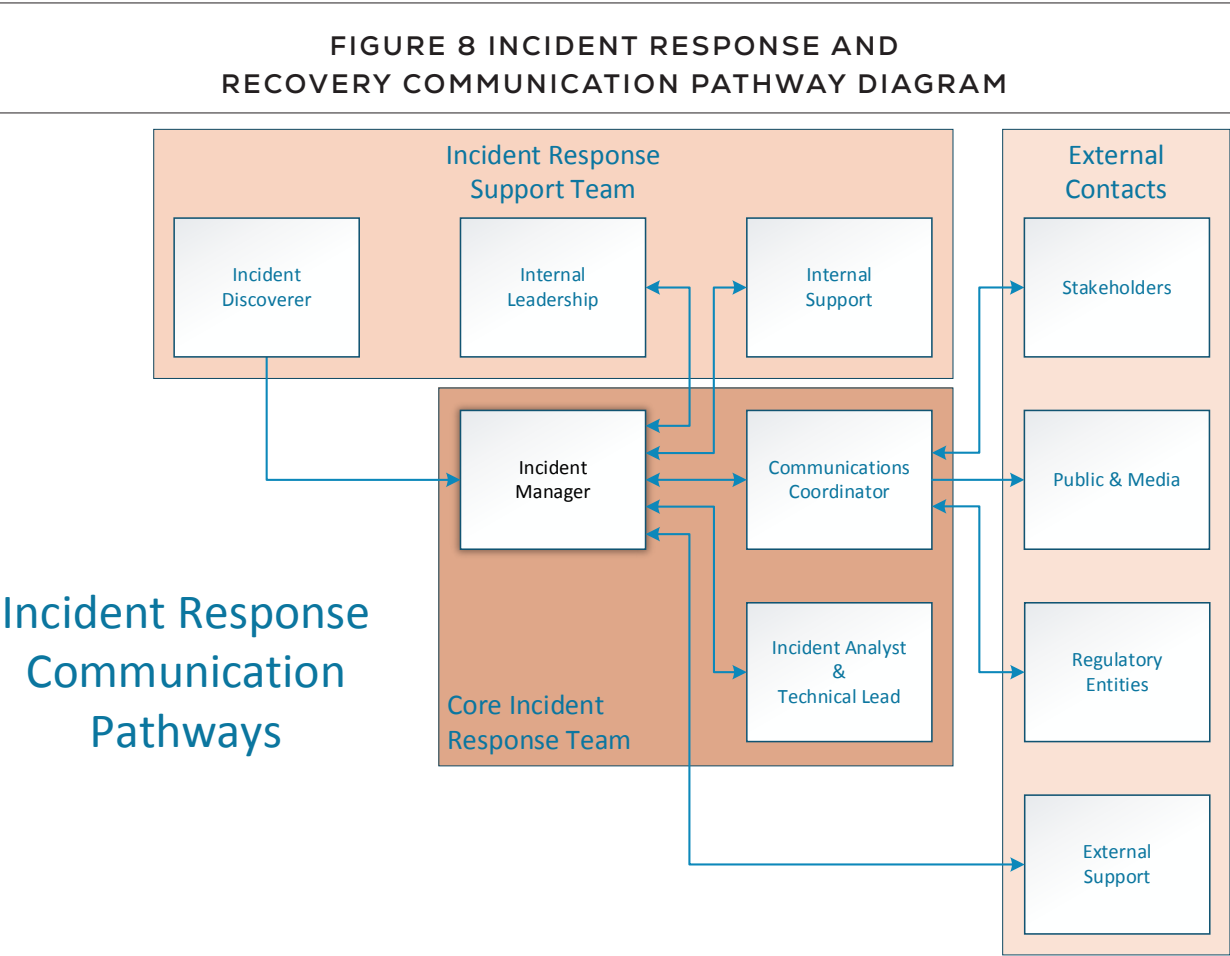
6.6 RESPONSE AND RECOVERY PLAN

A response and recovery plan was developed for the District and refined through collaborative workshops to tailor it to the District. The Response and Recovery Plan was provided to the District as a separate document. The integration effort of this Response and Recovery Plan has been defined in the project recommendations section of this SMP.

6.6.1 Incident Response Communication

Pathways

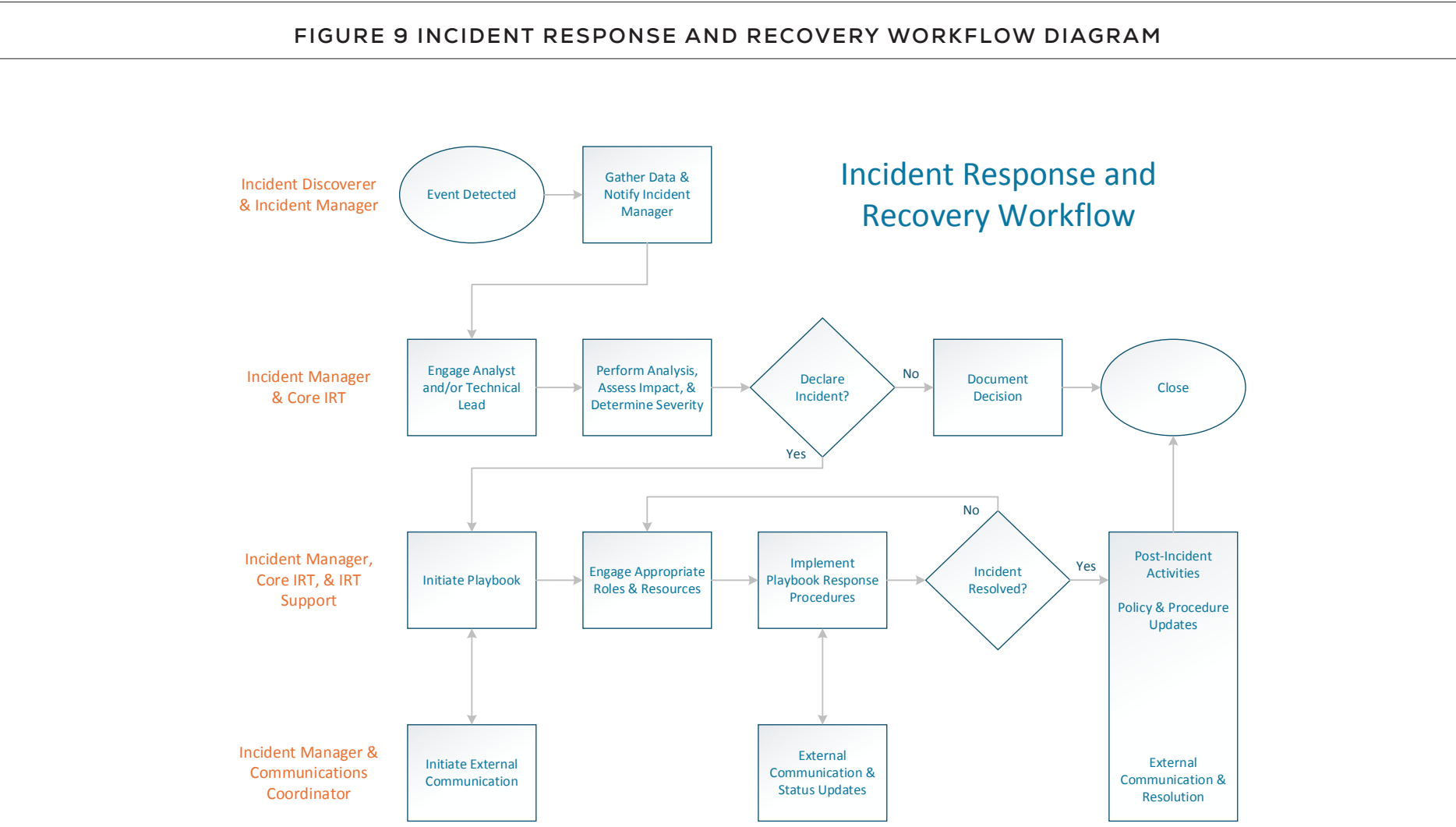
A summary diagram of the incident response and recovery communication pathways is provided below.



Incident Response Communication Pathways

6.6.2 Incident Response and Recovery Workflow

A summary diagram of the incident response and recovery workflow is provided below.





7 | SYSTEM GAP ANALYSIS

The existing system configuration details, infrastructure assessments, asset lists, system architecture, and the needs assessment information were used to identify gaps and obstacles that need to be addressed in order to transition from the current system to one that meets the District's current and future expectations.

7.1 SCADA

7.1.1 Software Reliability, Redundancy, and Long-Term Support

7.1.1.1 Identified Gaps

- › Operators have observed intermittent SCADA system slowdowns at HQ and are concerned about the system's ability to consistently support operations and timely alarm or event responses.
- › The Historian at HQ is a single instance and does not have redundancy or failover capabilities to reliably support critical operations and ensure data availability and integrity during failure conditions.

7.1.1.2 Identified Solutions

- › Architect and incorporate a robust and high availability SCADA solution at HQ with predictable performance characteristics to ensure reliable monitoring and control of critical processes.
- › Architect and incorporate a redundant Historian solution at HQ with automatic failover and recovery capability, including options such as mirrored databases, hot standby instances, or

cloud-based replication to support continuity of operations during hardware, software, or network failures.

7.1.1.3 Identified Standards

- › Future system planning should prioritize robustness, predictable performance, and high availability to ensure reliable monitoring and control of critical processes.
- › Future system planning should account for the trend towards subscription-based licensing and consider the long-term implications of licensing models, including cost predictability, scalability, & vendor support.
- › The District does not have a documented standard reflecting either system at the HQ or OPR plants, but the standard in practice at OPR is consistent with the prior integrator's standard, and is preferred over the legacy HQ standard in practice.
- › Local SCADA manufacturer support and familiarity with the Wonderware platform remain important considerations in evaluating current and future SCADA platform options, and the District would like to consider AVEVA as the SCADA platform at HQ to replace the current Intouch solution.

7.1.2 Historian Data Analysis Tools & Data Integration

7.1.2.1 Identified Gaps

- › Producing process data reports is largely manual, relying on Historian Client Tools, Excel spreadsheets, and daily manual sample data to generate regulatory state

reports. This approach increases the level of effort and introduces opportunities for errors and inconsistencies.

- › Additional process and system information is not currently captured or stored to support analytics, reporting, and post-event troubleshooting.
- › Many tags are not configured for storage in the Historian due to licensing constraints, limiting the ability to perform meaningful post-analysis and requiring Historian Client Tools like trending for troubleshooting and process monitoring activities.
- › User attributions are not currently tracked to support nonrepudiation and audit requirements.

7.1.2.2 Identified Solutions

At the HQ plant:

- › Implement a solution to automate Historian data collection as part of a unified reporting or data management platform that includes manually collected data to streamline state reporting and reduce manual data handling.
- › Consider options for moving collected daily manual data into SCADA to further support an automated reporting solution.
- › Evaluate and consider additional and appropriate process and system information for capture and storage to support analytics, reporting, and post-event troubleshooting.
- › Ensure appropriate sizing (licensing & storage) considerations and performance headroom are factored into Historian planning that accounts for a significantly

expanded tag set (including process, PLC health, I/O status, and other diagnostic data) with high-resolution data over appropriate time horizons to enable more effective root cause analysis, reporting, and system optimizations. › Identify a solution for tracking user attributions to support nonrepudiation and audit requirements, including when data is manually entered. › When possible, incorporate implemented solutions at the OPR plant for consistency, which appears to have a reporting server VM, though it is not clear what the exact process is for producing reports.	SmartSights XLReporter, which is used for SCADA and state-based reporting. › The ability to capture who entered or modified manual data will be an important consideration in evaluating any proposed solutions. › Any solutions should account for being able to work with a redundant Historian configuration and always use data from the active Historian instance and database.	› Make alarms be more specific, actionable, and better aligned with identifying the primary fault. › Implement alarm suppression or dependency logic where appropriate, so that secondary or consequential alarms do not obscure the primary causes of system failures. › Expand diagnostic data with PLC health, I/O module status, and other indicators to provide more insight into field process infrastructure and improve troubleshooting and root cause analysis beyond AC & DC power fail alarms. › When possible, incorporate implemented solutions at the OPR plant for consistency.	› The current system lacks flexibility and makes implementing changes difficult, and the District experiences challenges accessing and modifying the system across multiple layers, including SCADA, networking, and PLC programming, which limits its ability to respond quickly to operational needs.	though is not the primary factor.	all critical SCADA systems and system storage on an unlicensed version of VMware vSphere that doesn't offer HA, automatic recovery, or sharing of computing and storage resources. › Creation and storage of specific configurations and historical data is a manual process to a local NAS. › OPR infrastructure may be approaching end of life by the time a new HQ system is designed and integrated. › The OPR SCADA system has no local storage, and the backup strategy and location of critical configurations and VMs is not known.
7.1.2.3 Identified Standards › The current SCADA platform is Wonderware Intouch at HQ, and at OPR is the AVEVA System Platform. › The current SCADA Historian platform for both plants is Wonderware Historian. › The choice of underlying database technology is an important factor in determining how easily additional data sources can be integrated with SCADA in the future, and AVEVA continues to offer a SQL-based Historian platform, which is similar to the District's existing Historian implementation. › The District has identified Hach WIMS as a potential solution for managing manually collected and laboratory data; since Hach WIMS supports SQL-based databases, maintaining a SQL-based Historian architecture may provide advantages in terms of data integration, interoperability, and long-term analytics options. Hach WIMS also supports integration with	7.1.3 System Alarming & Notifications 7.1.3.1 Identified Gaps › During certain events, numerous alarms are triggered simultaneously, making it difficult to identify the true cause of issues. Secondary and consequential alarms often obscure primary causes of system failures. › Alarms aren't specific enough, actionable, or aligned well with primary faults. › SCADA doesn't have diagnostic information for PLC health, I/O module status, and other indicators that can provide deeper insight into the field process infrastructure beyond AC and DC power fail alarms. › When Apartis Lab Analyzer readings are transferred into SCADA using LinkMaster, values exceeding defined thresholds can initiate an automatic plant shutdown. 7.1.3.2 Identified Solutions At the HQ plant: › Eliminate or significantly reduce the use of "common" alarms.	7.1.3.3 Identified Standards › TopView is used for notifications via SMS (+ VOIP at OPR), which has proven more reliable than WIN-911. › Third-party solutions preferred for offering more stability, richer notification features, & greater flexibility. › District is comfortable continuing with SMS-based notifications & doesn't require voice-based alerting › SCADA access and integration plans should include Apartis Lab Analyzer data provided by packaged system vendors at the FBR treatment plant to ensure operators have reliable and timely visibility into analyzer status, data quality, shutdown conditions, and associated alarms.	7.1.4.2 Identified Solutions › The District would like to increase its level of independence in maintaining and modifying the system; training may facilitate this, and the District is also open to hiring a dedicated OT resource with broad integration skills and experience need to effectively support and maintain the OT environment given its size. › The District is interested in undertaking SCADA application development to facilitate self-reliance, and would like to consider training options to support this effort. › The District would like to incorporate the existing cybersecurity response plan into a comprehensive SCADA system response and recovery plan, ensuring it addresses broad infrastructure failure scenarios. 7.1.4.3 Identified Standards › Future solutions should emphasize improved accessibility, clearer system ownership, and reduced reliance on external resources for routine configuration changes, troubleshooting, and enhancements. › The ability for the District to be self-reliant in basic SCADA application development should be considered when selecting a SCADA platform,	7.1.5 User Interface 7.1.5.1 Identified Gaps › The District prefers using tablets and smartphones to interface with HQ SCADA, but the existing system was not developed to prioritize the use of SCADA on mobile devices like smartphones and tablets. 7.1.5.2 Identified Solutions › Investigate solutions for interfacing with HQ SCADA using tablets and smartphones like at OPR. › Ensure applications interfacing with HQ SCADA designed to support smaller mobile devices continue to work seamlessly with larger devices that use a keyboard & mouse, like panel mount PC's and client workstations. 7.1.5.3 Identified Standards › The District wants to use mobile clients with the HQ SCADA system to support operators at remote sites rather than solely localized clients, similar to the OPR SCADA solution designed to support mobile tablets.	7.2.1.2 Identified Solutions › HQ needs a modern SCADA system solution with active support providing HA, automatic recovery, sharing of computing & storage resources, and support for software redundancy, failover, and recovery; system design, integration, and initial and ongoing support costs must take the OPR plant into account (which may be near EOL by the time HQ is updated) with the goal being parity in hardware and software between the two plants. › Subscription-based licensing options will be evaluated to determine whether multi-year agreements can help manage and predict costs over time between both plants. › HQ needs a resilient backup and storage solution that provides automatic backups of configurations and historical data. › The OPR backup solution needs review to ensure it provides the

same level of resiliency as the solution designed for HQ.					
7.2.1.3 Identified Standards › The District strongly desires to standardize on as many components as practical within and across both plants, including hypervisors, network equipment, server and service deployments, and client systems. › The District is comfortable standardizing on the Dell VRTX platform for HQ to simplify management, but is open to other redundant server/storage solutions like Penguin (formerly Stratus) that must include parallel planning, design, and implementation considerations with the OPR plant for parity. › The District would prefer to continue using VMware due to their familiarity with it and existing infrastructure.	until they impact other systems. › No confirmation of UPS testing or monitoring is mentioned at either plant. › The existing HQ and OPR plants are not architected with consideration of “split-brain” risk and have both primary and secondary SCADA components co-located in the same location.	monitoring and notifications for SCADA infrastructure with solutions that leverage common protocols, such as SNMP. › HQ is planned for relocation to FBR (most likely) or OPR in the next 5 years. › The OPR plant is being considered for redundant secondary components and/or for an Emergency Operations Center (EOC) to support system response and recovery operations. › Redundancy planning should balance operational availability, recovery time objectives, and risk mitigation for both planned and unplanned outages.	› Include architecture decisions that provide traffic-shaping configuration in the firewall solution at HQ to parallel OPR design. › Design and implement a standardized network segmentation approach for the HQ and OPR facilities that supports all required asset types at both locations, applies appropriate isolation principles, and establishes a consistent standard for network segmentation across current and future District OT environments.	7.2.4.3 Identified Standards › The District is open to forward-looking strategies enhancing the reliability of remote site communications, including specifying radio hardware with cellular backup, which also provides flexibility for secondary SCADA or EOC sites and reduces dependence on radio communications from specific locations, as HQ does now. › At a minimum, critical sites should be considered for future cellular backup communications.	› PLC programs at HQ do not provide sufficient diagnostic data (PLC health, I/O module status, Intrusion) to the SCADA system, limiting operators’ ability to quickly identify and respond to field device or controller issues before they escalate into process disruptions. › PLC alarm logic at HQ relies heavily on common or grouped alarms that do not clearly distinguish primary faults from secondary or consequential conditions, reducing alarm specificity and actionability consistent with the SCADA alarming gaps identified in Section 7.1.3. This is critical for root cause analysis of equipment failure or process inadequacies. › There is no formal PLC program version control, change management, or backup verification process at either facility; the current state of running programs may not match available backup copies, and there is no established process to verify program integrity or recover from unauthorized or unintended changes. › Certain process control relationships depend on SCADA to redirect data between peers; for example, RTU-29 monitors RTU-17’s flow via SCADA redirection. However, best practice recommends enabling direct communication between these peers, thereby reducing reliance on the operational status of SCADA for proper functionality. › Remote sites lack standardized basic security features monitored by the PLC, such as intrusion detection at electrical panels and site access, as well as unique passwords for all programs.
7.2.2 Platform Environment, Monitoring, & Operational Redundancy 7.2.2.1 Identified Gaps › Core SCADA infrastructure and operator workstations at HQ are co-located in a single control room, which is somewhat cramped, with its use for multiple purposes contributing to clutter and congestion. › Core SCADA infrastructure in the equipment rack at OPR is full of construction dust and debris. › Neither the environmental conditions (temperature, humidity) nor the infrastructure components themselves are actively monitored at either plant, and failures may go unnoticed	7.2.2.2 Identified Solutions › Develop short-term and transitional plans to separate core SCADA infrastructure from operator workstations at HQ and the future plant location and ensure each area has enough space and is free from clutter. › Implement protective measures for the core SCADA infrastructure at OPR to protect from dust and debris. › Develop and implement solutions for monitoring and notification of environmental conditions and SCADA infrastructure at HQ, OPR, and future plant locations that leverages common (non-proprietary) protocols. › Develop policy and procedures for UPS testing and monitoring at all plants. › Architect and implement a solution for SCADA infrastructure that considers “split-brain” risk and distributes redundant components for failure/failover scenarios at secondary sites and a third location for cold backup and disaster recovery; include associated policies and procedures to backup and recovery plans. 7.2.2.3 Identified Standards › The District is interested in improving	7.2.3 Core Networking 7.2.3.1 Identified Gaps › Both HQ and OPR plants lack redundancy in critical network infrastructure like OT firewalls and core switches. › The HQ system does not implement traffic-shaping policies in the firewall like the OPR system does. › The HQ network supports fewer assets than OPR but employs more appropriate and well-defined network segmentation, whereas the OPR network lacks sufficient segmentation in several key areas despite supporting a significantly larger and more diverse set of assets. 7.2.3.2 Identified Solutions › Design an implement HA network solutions at HQ and OPR that includes firewalls, routers, core switches, and associated device connectivity that allows for zero-downtime maintenance and automatic failover scenarios.	7.2.3.3 Identified Standards › The District needs standardized solutions and parity across plants for core networking, traffic management, and network segmentation. 7.2.4 Telemetry 7.2.4.1 Identified Gaps › The HQ system lacks communication redundancy between both critical and non-critical plant sites for the existing 900 MHz serial RF network. 7.2.4.2 Identified Solutions › The District is interested in licensed ethernet radios with a backup cellular option to provide redundancy for critical remote sites in the HQ system. Non-critical remote sites will operate on licensed ethernet radio only. › Higher bandwidth requirements need to be factored into cellular redundancy solutions for AVEVA and VT SCADA, including accounting for primary and secondary distribution across sites.	7.2.5 PLC & Process Control 7.2.5.1 Identified Gaps › The HQ distribution system relies on Tesco LIQ PLCs, which are proprietary, legacy hardware available exclusively through Tesco Controls; this creates a single-source vendor dependency for hardware procurement, replacement parts, firmware support, and programming services, and presents a significant long-term supportability and supply chain risk. › Multiple generations of Tesco PLCs are deployed across HQ remote sites, resulting in inconsistent hardware capabilities, varying programming environments, and increased complexity for maintenance and troubleshooting . › The HQ and OPR facilities operate on entirely different PLC platforms (Tesco LIQ at HQ vs. Allen-Bradley ControlLogix at OPR), preventing standardization of hardware, programming tools, spare parts inventories, and staff training across the District.	

7.2.5.2 Identified Solutions

- › Develop a phased migration plan to replace the legacy Tesco LIQ PLCs with a modern, industry-standard PLC platform, prioritizing critical and highest-risk sites first
- › Utilize standardized Add-On Instructions (AOIs) or user-defined function blocks for motor control, valve control, analog instrument processing, alarm logic, and PID control to promote consistency and reduce integration risk during migration that is manageable for staff to maintain in the future.
- › Expand PLC-to-SCADA diagnostic data to include PLC processor health, I/O module fault status, communication link status, and equipment runtime counters to improve operational visibility and support proactive maintenance.
- › Redesign PLC alarm logic to eliminate common or grouped alarms and implement specific, actionable, and prioritized alarm points with appropriate on-delay timers, deadbands, and alarm suppression or dependency logic to reduce nuisance alarms and improve fault identification
- › Replace legacy serial communication protocols with industry-standard industrial Ethernet protocols as part of the PLC platform migration to support modern SCADA integration and improved data throughput.
- › Develop and adopt a comprehensive, District-owned PLC Programming Standards document covering program architecture, tag naming conventions, I/O processing, alarm logic, process

control conventions, communications, documentation requirements, and change management procedures

- › Document existing process control narratives for all PLC-controlled processes at both facilities and update them to reflect any changes made during the PLC migration or standardization effort
- › Provide District staff with training on the standardized PLC platform and programming tools to support increased self-reliance for routine PLC maintenance, troubleshooting, and minor program modifications.
- › Replace data transmitted via SCADA redirection with direct peer to peer communication.
- › Standardize PLC-monitored physical and logical security at remote sites by implementing intrusion detection for electrical panels and site access upon site improvement. Require unique PLC program passwords and consistent access control practices across all remote facilities.

7.2.5.3 Identified Standards

- › The District strongly desires to standardize on PLC hardware platforms and associated I/O architectures across both plants to improve consistency, supportability, and long-term maintainability.
- › PLC programming shall be performed in a consistent, agreed upon manner and structure, to support readability and maintainability by District staff.
- › Future PLC programming and process

control design shall prioritize District self-reliance by using standardized, well-documented program structures, reusable function blocks, and comprehensive inline documentation sufficient for qualified District staff to maintain and troubleshoot the system without external integrator dependency for routine tasks.

- › Process control narratives shall be documented for all PLC-controlled processes at both facilities and maintained as living documents that are updated to reflect any changes made during the PLC migration or future system modifications.
- › Remote sites shall incorporate standardized PLC-monitored physical and logical security, including intrusion detection for electrical panels and site access, unique PLC program passwords, and consistent access control practices across all facilities.

7.2.5.4 HQ

The PLCs that make up the process control system primarily run as standalone programs for wells, boosters, and intertie sites. Some peer-to-peer communication is supported by a PLC (RTU-99) located at HQ. Additionally, the FBR plant has dedicated PLCs that operate independently and are not part of the larger HQ System.

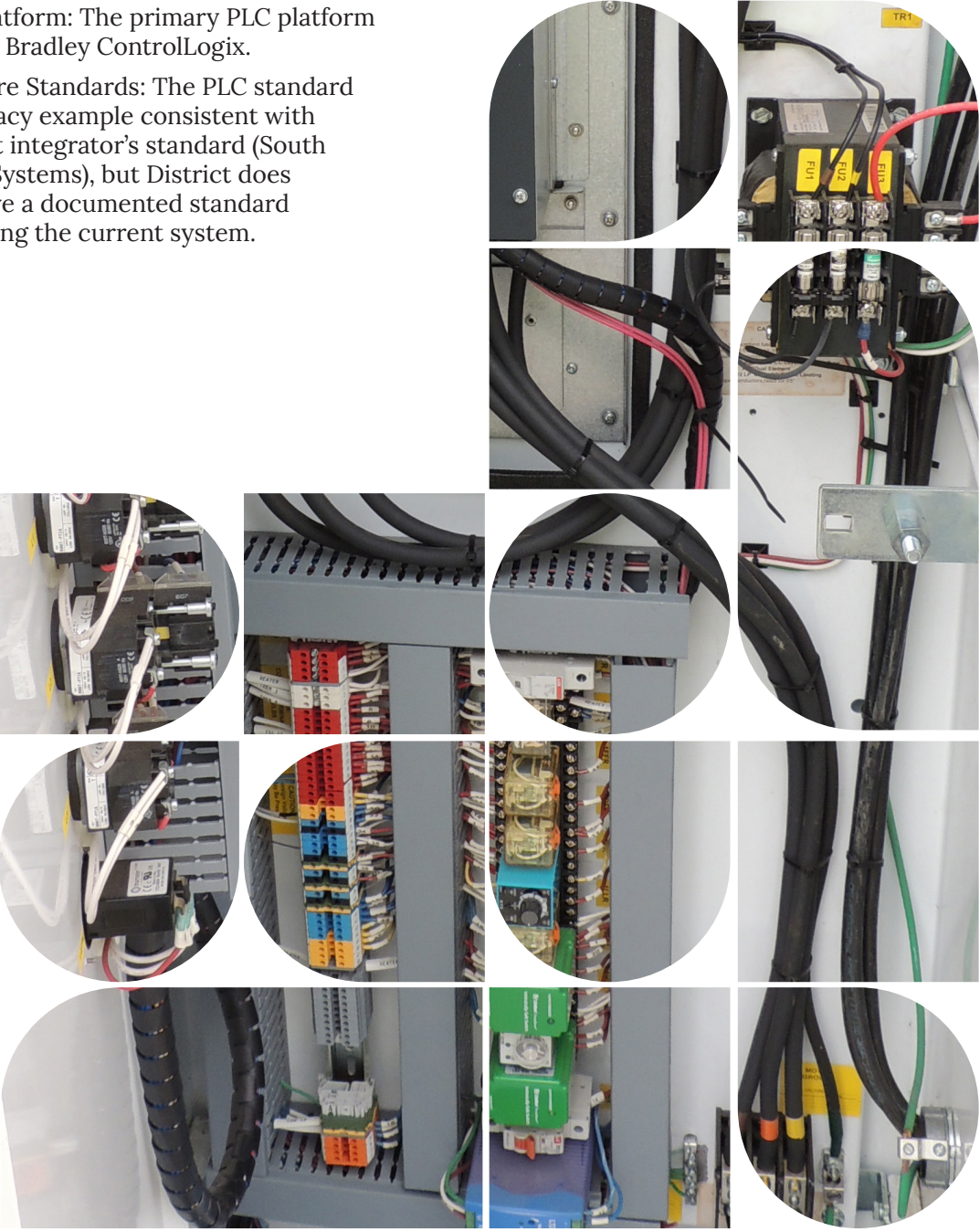
- › PLC Platform: The primary PLC platform is Tesco LIQ's; there are multiple different generations of Tesco PLC's, all of which are legacy models that are proprietary in nature – only Tesco controls services and provides Tesco LIQ PLC's.

- › Software Standards: The PLC standard is a legacy example consistent with prior integrator's standard (Tesco Controls), but District does not have a documented standard reflecting the current system.
- › Process Control: The process control narratives for the PLCs are provided in Companion Document D.

7.2.5.5 OPR

The PLCs that make up the process control system are distributed throughout various areas of the plant and are dedicated to specific processes. A main PLC is configured with redundant CPUs in a hot/standby arrangement; notably, the primary and secondary PLC nodes are installed in separate buildings and are separated by a significantly greater distance than is typically encountered for redundant CPU configurations. Most PLCs operate as standalone programs supporting wells, boosters, and intertie sites. Limited peer-to-peer communication is supported by a PLC (RTU-99) located at HQ. Additionally, the FBR plant has dedicated PLCs that operate independently and are not part of the larger HQ System.

- › PLC Platform: The primary PLC platform is Allen Bradley ControlLogix.
- › Software Standards: The PLC standard is a legacy example consistent with current integrator's standard (South Coast Systems), but District does not have a documented standard reflecting the current system.





8 | SYSTEM DESIGN CRITERIA

The system design criteria has been developed from the sum of all information collected, reviewed, workshopped, and established as the criteria for future District projects.

8.1 SOFTWARE STANDARDS

8.1.1 Software Documentation Standards

The District does not currently maintain a documented SCADA system standard applicable to either the HQ or OPR facilities. In practice, the SCADA system implementation at the OPR facility follows the prior system integrator's standard and is considered the District's preferred approach.

- › Future SCADA system design at HQ and other District facilities shall align with the OPR implementation standard, rather than the legacy HQ practices, unless otherwise justified and approved by the District.

8.1.2 SCADA

The District's existing SCADA platforms include Wonderware InTouch at Headquarters (HQ) and AVEVA System Platform at the OPR facility.

8.1.2.1 Platform Standardization

- › Future SCADA system design shall consider standardization on the AVEVA System Platform to improve system consistency, long-term supportability, and integration across District facilities.

- › Local system integrator support availability and District staff familiarity with the Wonderware/AVEVA ecosystem shall be considered key factors in platform selection and system design.

8.1.2.2 Modernization

- › The HQ SCADA system shall be designed to replace the existing Wonderware InTouch solution with an AVEVA System Platform-based architecture.
- › The proposed architecture shall support scalable system expansion and future integration with additional facilities, subsystems, and data consumers.

8.1.2.3 Mobile and Remote Operations

- › The HQ SCADA system shall support secure mobile SCADA clients to enable operational access for authorized users at remote facilities.
- › Mobile access shall be designed to reduce reliance on fixed, localized operator workstations and provide functionality comparable to the OPR SCADA system, including support for tablet-based operation.
- › Mobile client implementation shall comply with District cybersecurity policies and industry best practices.

8.1.2.4 System Performance and Availability

- › The SCADA system shall be designed for high availability, including redundancy at the server, network, and application levels as appropriate.
- › System performance shall be predictable under normal and peak operating

conditions, with sufficient capacity to support concurrent users, mobile clients, and data historian functions.

- › The system shall provide robust alarm management, event logging, and fault tolerance to ensure continuous monitoring and control of critical processes.

8.1.2.5 Licensing and Lifecycle Considerations

- › SCADA system design shall account for current and anticipated trends toward subscription-based licensing models.
- › Licensing strategies shall be evaluated to ensure long-term cost predictability, scalability, and alignment with District budgeting practices.
- › Vendor support models, upgrade paths, and long-term platform viability shall be considered as part of the overall system lifecycle planning.

8.1.3 Historian & Data Integration

The current SCADA Historian platform at both the HQ and OPR facilities is Wonderware Historian.

8.1.3.1 Historian Platform and Architecture

- › The SCADA Historian solution shall be based on a SQL-based database architecture.
- › The Historian platform shall be compatible with the District's existing Wonderware Historian data model and support migration or coexistence as required.

› The Historian solution shall support integration with AVEVA SCADA platforms and associated data services.	redundant Historian instances.	with District authentication mechanisms where applicable.	demonstrate proven reliability in production SCADA environments.	and Maintenance Independence	minimize reliance on external resources for routine troubleshooting, minor enhancements, and system maintenance.
8.1.3.2 Data Integration and Interoperability › The Historian system shall support integration with external data sources, including manually collected operational data and laboratory data management systems. › The Historian system shall be compatible with Hach WIMS and support SQL-based data exchange mechanisms to facilitate bidirectional data integration where required. › The Historian system shall support integration with SmartSights XLReporter for SCADA reporting and regulatory or state-based reporting. › The Historian system shall allow authorized third-party analytics and reporting tools to access historical data without compromising system performance or security.	8.1.3.4 Manual Data Entry and Management › The system shall support the entry of manually collected and laboratory data through secure user interfaces. › The system shall allow manual data entry from authorized users and defined user roles only. › The system shall support validation rules, range checks, and required fields for manually entered data.	8.1.4 Notifications & Alerting TopView is used for notifications via SMS (+ VOIP at OPR), which has proven more reliable than prior WIN-911 product utilized by the District.	8.1.4.3 Alarm Management and Integration › Alarm notifications shall be generated based on SCADA alarm states and priorities. › The system shall support filtering and suppression of nuisance alarms to prevent alert fatigue. › The notification system shall maintain logs of alarm delivery, acknowledgment, and escalation activity for audit and troubleshooting purposes.	8.1.5.1 Application Development and Configuration › The selected SCADA platform shall support District staff performing basic SCADA application development tasks, including configuration changes, graphics updates, alarm adjustments, and tag management. › The SCADA system shall provide configuration tools and workflows that are accessible to appropriately trained District personnel without requiring vendor-specific programming for routine tasks. › Advanced customization or specialized development may be performed by external integrators; however, routine configuration changes shall not require third-party support.	› System documentation, including application architecture, configuration standards, and operational procedures, shall be provided to enable effective knowledge transfer to District staff. › The platform shall support version control, backup, and restore capabilities to allow District staff to safely manage and recover SCADA application changes.
8.1.3.3 Redundancy and High Availability › The Historian architecture shall support a fully redundant configuration, including primary and secondary Historian instances. › The system shall automatically direct data access and write operations to the active Historian instance and associated database without requiring manual operator intervention. › The Historian system shall maintain data continuity and prevent data loss during failover events between	8.1.3.5 Auditability and Data Traceability › The system shall capture and store the identity of the user who entered or modified manual data. › The system shall record timestamps for all manual data entry and modification events. › The system shall retain both original and modified values for manually entered data to support full audit trails. › The system shall provide query and reporting capabilities to retrieve audit trail information for review, compliance, and troubleshooting purposes.	8.1.4.1 Alarm Notification Platform › The SCADA system shall support integration with third-party alarm notification platforms. › Alarm delivery via SMS messaging shall be a requirement of the alarm notification solution. › Voice-based alarm notifications shall not be required as part of the alarm notification solution. › The notification solution shall provide reliable delivery of alarm messages to authorized users with acknowledgment capability. › The notification platform shall support configurable escalation rules, on-call schedules, and alarm prioritization. › The notification platform shall operate independently of SCADA HMI clients to ensure alarm delivery during client or workstation outages.	8.1.4.4 Analyzer Data Visibility and Integration › The SCADA system shall provide real-time visibility of Apartis Lab Analyzer data from the FBR plant. › Analyzer data shall be available to operators through all SCADA access methods, including local HMIs, mobile clients, and remote access solutions. › The SCADA system shall display analyzer status, data quality indicators, and analyzer-initiated shutdown or fault conditions. › The SCADA system shall generate alarms for analyzer faults, data quality issues, and shutdown conditions with appropriate priority levels. › Integration of analyzer data provided by packaged system vendors shall be included in all SCADA design, access, and integration plans.	8.1.5.2 System Accessibility and Usability › The SCADA system shall provide intuitive user interfaces for both operations and system configuration to support efficient day-to-day use and maintenance. › System access shall support role-based permissions to clearly define system ownership, responsibilities, and authorized actions. › The system shall support secure remote access for authorized District staff to perform monitoring, troubleshooting, and configuration tasks.	8.1.5.4 Long-Term Maintainability › The SCADA solution shall support a clear and maintainable application structure to facilitate long-term system evolution. › The system shall support scalable design practices to accommodate future expansion without requiring fundamental redesign. › Vendor and integrator dependencies shall be minimized through the use of standardized tools, open interfaces, and widely supported technologies.
	8.1.3.6 Security and Access Control › The Historian and associated data entry systems shall support role-based access control. › The system shall restrict data entry, modification, and approval privileges based on assigned user roles. › The system shall support integration	8.1.4.2 Third-Party Notification Solutions › Third-party alarm notification solutions shall be preferred over native SCADA notification tools where they provide improved stability, feature richness, and configuration flexibility. › The proposed solution shall		8.1.5.3 Operational Independence › The SCADA platform shall be designed to	
			8.1.5 Administration		

future SCADA, server, and network deployments unless deviations are approved by the District. › Any proposed deviations from the OPR standard shall be clearly identified, technically justified, and documented.	consistent with industry best practices for industrial control systems. › Core network services (e.g., routing, switching, firewalling, VLANs, and traffic control) shall be implemented consistently across plants to support predictable performance and security posture.	Proposed server and storage solutions shall support redundant components and fault-tolerant operation appropriate for critical SCADA workloads.	lifecycle management consistent with District operational requirements.	› The monitoring solution shall provide dashboards and reporting suitable for both operations and technical support staff. › Monitoring and alerting shall be designed to minimize nuisance alarms and support timely identification of infrastructure issues impacting SCADA availability.	and recovery capabilities sufficient to meet defined operational availability and recovery time objectives (RTOs).
8.2.1.2 Infrastructure Standardization The District shall standardize infrastructure components to the greatest extent practical across both HQ and OPR facilities. Standardized components shall include, but are not limited to: › Hypervisor platforms › Network equipment (Firewalls, switches, routers, modems, etc.) › Server hardware and operating systems › Virtual machine configurations and service deployments › SCADA server roles and application services › Client systems, including operator workstations and mobile clients Infrastructure designs shall prioritize consistency to simplify support, maintenance, training, and lifecycle management.	8.2.1.4 Scalability and Future Expansion › Standardized infrastructure and network solutions shall support future system expansion, additional facilities, and evolving operational requirements without requiring fundamental redesign. › The design shall support the addition of new SCADA services, data consumers, and integration points while maintaining standardized deployment patterns.	8.2.2.2 Parity and Standardization Across Plants › Server and storage architectures shall be designed to maintain functional and operational parity between the HQ and OPR facilities wherever practical. › Differences between HQ and OPR implementations shall be minimized and clearly documented when unavoidable.	8.2.3 Monitoring & Notification 8.2.3.1 Infrastructure Monitoring › The SCADA system infrastructure shall support centralized monitoring of servers, virtual machines, network devices, and core SCADA services. › Monitoring solutions shall leverage industry-standard protocols, including SNMP, wherever supported by the underlying infrastructure. › The monitoring system shall provide visibility into infrastructure health, availability, resource utilization, and fault conditions. 8.2.3.2 Notifications and Alerting › Infrastructure monitoring solutions shall support configurable notifications for abnormal conditions, performance thresholds, and failures. › Notifications shall be capable of integrating with the District's preferred notification mechanisms, including SMS-based alerting. › Alerting shall support prioritization, escalation, and acknowledgment workflows. 8.2.3.3 Integration with SCADA Operations › Infrastructure monitoring shall operate independently of SCADA application alarms while supporting integration where beneficial for operational awareness.	8.2.3.4 Standardization and Expandability › The monitoring architecture shall be scalable to support future expansion of SCADA infrastructure and additional facilities. › The solution shall use open, well-supported protocols to reduce vendor lock-in and support long-term maintainability.	8.2.4.3 Redundancy and High Availability › SCADA system architecture shall include redundancy at critical layers, including servers, historians, network components, and core services. › Redundant system design shall balance operational availability, risk mitigation, and cost considerations for both planned and unplanned outages. › Redundancy planning shall ensure that failover processes maintain system integrity, data consistency, and continuity of operator visibility and control. › The system shall provide monitoring and alerting for failover events and redundant system status.
8.2.1.3 Network Architecture and Parity Across Plants › The SCADA network architecture shall be standardized across plants to provide parity in core networking, traffic management, and network segmentation. › The network design shall support defined security zones and conduits	8.2.2 Virtual Servers, Storage, and Platform 8.2.2.1 Server and Storage Platform The District shall consider standardizing on the Dell VRTX platform for the HQ facility to simplify system management and operations. Alternative redundant server and storage solutions (e.g., Penguin Computing/formerly Stratus) may be proposed, provided they support equivalent or improved availability, performance, and maintainability. Any alternative server or storage solution shall be evaluated in parallel with the OPR plant infrastructure to ensure architectural parity, operational consistency, and long-term supportability across facilities.	8.2.2.3 Virtualization Platform › The SCADA system shall be deployed on a virtualization platform. › VMware shall be the preferred virtualization platform based on District familiarity and existing infrastructure. › Any proposed alternative virtualization platform shall demonstrate clear advantages and be approved by the District prior to implementation. › The virtualization environment shall support high availability, snapshotting, backup, and recovery of SCADA system components. 8.2.2.4 Lifecycle and Support Considerations › Server, storage, and virtualization solutions shall be supported by vendors with proven experience in industrial and SCADA environments. › Solutions shall support long-term vendor support, patching, and	8.2.3.4 Standardization and Expandability › The monitoring architecture shall be scalable to support future expansion of SCADA infrastructure and additional facilities. › The solution shall use open, well-supported protocols to reduce vendor lock-in and support long-term maintainability.	8.2.4 Redundancy 8.2.4.1 HQ Relocation Planning › The SCADA system design shall account for the planned relocation of the HQ facility within the next five years, most likely to the FBR site, with OPR as an alternative. › Relocation plans shall address continuity of operations, system availability, and minimal disruption during the transition. 8.2.4.2 Secondary/Redundant Facilities › The OPR facility shall be evaluated as a site for redundant secondary SCADA components and/or as an Emergency Operations Center (EOC) to support system response and recovery operations. › Redundant systems shall support failover	8.2.4.4 Operational Continuity and Recovery › SCADA system design shall support recovery objectives that align with District operational priorities, including continuity of critical processes and timely restoration of full system functionality after disruption. › Emergency Operations Center functionality shall provide remote access to critical SCADA components for authorized personnel during incidents, outages, or relocation activities. › Relocation and redundancy planning shall be documented, tested, and validated as part of routine operational and disaster recovery exercises.

8.2.5 Telemetry

8.2.5.1 Communication Reliability and Redundancy

- › The SCADA system design shall incorporate strategies to enhance the reliability of communications with remote sites.
- › Critical remote sites shall be provisioned with redundant communication pathways to ensure continued SCADA connectivity in the event of primary network or radio failures.
- › Redundant communication options shall include cellular backup, satellite links, or other reliable technologies as appropriate.

8.2.5.2 Radio and Cellular Integration

- › Radio hardware selected for remote site communications shall support cellular backup to reduce dependence on any single communication medium.
- › The system shall enable flexibility to support secondary SCADA servers or Emergency Operations Center (EOC) operations from remote locations.

8.2.5.3 Future-Proofing and Expansion

- › The design shall allow for expansion of cellular backup communications to additional remote sites beyond critical sites, as operational needs and budget allow.
- › Communication architectures shall be designed to accommodate future technologies and standards without requiring complete system redesign.

8.2.5.4 Operational Considerations

- › Redundant communication systems shall maintain sufficient bandwidth, latency, and reliability to support SCADA monitoring, control, and alarm notification requirements.
- › Failover between primary and backup communication paths shall be automatic or require minimal operator intervention and shall be logged for audit purposes.
- › Remote communication solutions shall comply with applicable cybersecurity and network segmentation standards to prevent unauthorized access.

8.3 FIELD ENCLOSURE STANDARDS

Field enclosure standards define the minimum requirements for all SCADA and control system enclosures installed at remote sites throughout the District. These standards are derived from the field assessment findings and are intended to ensure operator safety, equipment longevity, and compliance with applicable codes including UL508A, NFPA 70, and NEC.

Enclosure Construction and Type: All new field enclosures shall be NEMA Type 3R (or Type 12 for indoor installations) rated, constructed of galvanized steel or 304 stainless steel, finished in ANSI 61 Gray. Wallmount enclosures shall be sized to accommodate current equipment and allow a minimum 20% spare capacity for future expansion. Where multiple enclosures exist at a site (e.g., separate PLC and power supply enclosures), they shall be consolidated into a single enclosure where practical. Degrading backboards shall be replaced with

Unistrut-style mounting systems to improve equipment organization and serviceability.

Electrical Safety and Code Compliance: All control panels shall undergo short circuit current rating analysis and validation per UL508A requirements. AC voltage separation shall be maintained within all enclosures; where 480VAC and 120VAC coexist in the same panel, physical separation barriers and proper exterior labeling shall be installed. All enclosures shall include clear voltage identification labels on the exterior of the enclosure door indicating all voltage levels present. De-energization procedures shall be documented and posted for panels containing multiple voltage levels.

Surge Protection and Grounding: Surge Protection Devices (SPDs) shall be installed in all PLC control panels, MCC sections, and communication hardware enclosures. Lightning arrestors shall be installed per NFPA 70 Articles 810 and 820 for all antenna and coaxial cable installations. All coaxial cables shall be properly grounded. RFI filters shall be maintained in all enclosures to protect sensitive electronic equipment from electromagnetic interference.

Thermal Management: All new enclosures shall be equipped with cooling fans and filtered air intake to prevent dust intrusion and maintain acceptable operating temperatures. Existing enclosures with fans shall have filters inspected and replaced on a regular maintenance schedule. Fan filters shall be rated to prevent particulate ingress that can degrade electrical

component life. Heaters shall be provided in enclosures where condensation is a concern.

Security and Access Monitoring: All enclosures shall be equipped with intrusion switches connected to the PLC for SCADA-based door alarm monitoring. Nameplates shall be legible and include the RTU number, site designation, and enclosure contents. Nameplates may be installed on the interior of the enclosure door for security where external labeling poses a risk.

Internal Lighting and Maintenance Access: All enclosures shall include internal enclosure lighting to facilitate maintenance and troubleshooting. Duplex receptacles shall be provided for maintenance tool power. Wire labeling shall be comprehensive, covering both internal wiring and field wires, with legible and durable labels. Panels shall be cleaned on a regular preventive maintenance schedule to remove dust, debris, and biological contaminants that can degrade component life.

Backup Power Systems: Each enclosure shall include a standardized DC power supply with a charger and appropriately sized battery backup. The standard configuration shall consist of a 12VDC charger with 12V 18Ah sealed lead-acid batteries. UPS systems rated below 104°F shall be replaced with charger and battery configurations suitable for the outdoor operating environment. Batteries shall be replaced on a documented schedule not to exceed five years or as indicated by load testing.

8.4 PROGRAMMING STANDARDS

The following programming standards establish the design criteria for PLC-based control systems across all District facilities. These standards shall apply to all new PLC programming, retrofits, and modifications to existing control logic. The OPR facility’s existing PLC programming conventions shall serve as the reference baseline, where possible.

8.4.1 General PLC Programming Standards

- › All PLC programs should be developed in Ladder Diagram (LD) or Function Block Diagram (FBD).
- › Ladder Diagram shall be the primary programming language for discrete control logic, motor control, alarm processing, and equipment sequencing to support readability and maintainability by District operations and maintenance staff.
- › PLC programs should be programmed in the version of programming software that the District is currently using.
- › All PLC programs shall include descriptive tag names, comments, and routine descriptions sufficient for a qualified District representative to understand the intent and operation of the logic without requiring reference to external documentation.
- › Tag naming conventions shall follow a standardized naming schema that identifies the facility, process area, equipment, and signal type. The naming convention shall be documented in the PLC Programming Standards document and applied consistently across all District PLCs.

- › Setpoints, thresholds, timers, and configurable parameters shall be defined as named tags accessible from the SCADA system to support operational adjustments without requiring PLC program modifications.
- › PLC programs shall be designed to fail to a safe and known state upon loss of communications, loss of power, processor fault, or other abnormal conditions. Safe-state behavior shall be defined for each controlled process and documented in the process control narrative.

8.4.2 Program Architecture and Organization

- › PLC programs shall be organized into functionally separated routines or tasks consistent with WVWD programming standards.
- › Reusable logic shall be implemented as user-defined function blocks to promote consistency, reduce programming errors, and simplify maintenance. These should be implemented for commonly used functions including motor control, valve control, analog instrument scaling, PID control, and alarm processing.

8.4.3 I/O Processing Standards

- › All physical I/O shall be read and written through dedicated I/O processing routines at the beginning and end of each program scan cycle, respectively. Control logic shall reference internal mapped tags rather than direct I/O addresses to support simulation, testing, and troubleshooting.
- › Analog input signals shall be scaled from raw engineering units to process units

within the I/O processing routine. Scaling parameters, including zero and span values, engineering unit range, and signal type (4–20 mA) shall be configurable via named tags. › Analog input processing shall include signal validation logic to detect out-of-range conditions, sensor failures (open-circuit and short-circuit detection for 4–20 mA signals), and signal quality indicators. › Discrete inputs shall incorporate configurable debounce filtering to prevent false triggering from electrical noise or contact bounce. Debounce timer values shall be appropriate for the application and documented in the I/O configuration. › All I/O modules shall be configured to report module and channel-level faults to the PLC processor. I/O fault status shall be available to the SCADA system for diagnostic display and alarm generation. › Spare I/O capacity shall be provided at a minimum of 20% for each I/O type (discrete input, discrete output, analog input, analog output) per I/O chassis or remote I/O rack at the time of initial installation.	configurable high-high, high, low, and low-low alarm setpoints. Rate-of-change alarms shall be provided where process conditions warrant early detection of abnormal trends (for instance, rapid change of a reservoir level). › All alarm setpoints, deadband values, on-delay timers, and off-delay timers shall be configurable from the SCADA without requiring PLC program modifications. Alarm configuration changes shall be logged by the SCADA historian for audit purposes. › On-delay timers shall be applied to alarm conditions to prevent nuisance alarms from transient process fluctuations.	shall include configurable position deadband and rate-of-travel limiting. › PID control loops shall be implemented using the PLC platform's native PID instruction set. All PID loops shall support bumpless transfer between manual and automatic modes, anti-windup protection, and configurable output clamping. › Grouped equipment logic, including pump lead/lag rotation, duty/standby alternation, and sequential start delays, shall be implemented in a way consistent with District standards.
8.4.4 Alarm Logic Standards › Alarm detection shall be performed in the PLC rather than at the SCADA level to ensure alarm conditions are captured and acted upon regardless of SCADA communication status. Critical alarms shall initiate protective actions directly from PLC logic without dependency on SCADA commands. › Analog alarm processing shall support	8.4.5 Process Control Standards › All motor-driven equipment shall be controlled through a standardized motor control AOI or function block that provides uniform Local/Remote monitoring, run/stop control, run confirmation monitoring, fail-to-start and fail-to-stop logic, and runtime and motor starts accumulation. › Variable frequency drive (VFD) controlled equipment shall include speed command and feedback monitoring, drive fault detection and reporting. VFD communication status shall be monitored, and loss of communication shall trigger a defined fallback operating mode. › Valve control logic shall be implemented through a standardized valve control AOI or function block that supports open/close command, position feedback (for modulating valves), transit time monitoring, and failure-to-actuate alarms. Modulating valve control	8.4.6 Communications and Data Exchange › Communications between PLC and SCADA systems must utilize contemporary Industrial Ethernet protocols. Legacy serial protocols should be transitioned to Ethernet-based alternatives during system upgrades wherever feasible. › Communication status monitoring logic shall be included in every PLC program to detect and report loss of communication with the SCADA server, remote I/O racks, networked field devices, and peer PLCs. Communication loss shall trigger appropriate alarms and initiate defined fallback control behavior. › Heartbeat or watchdog mechanisms shall be implemented between the PLC and SCADA system to provide continuous verification of communication health. Stale data conditions shall be detected and flagged at both the PLC and SCADA levels.

8.4.7 Program Documentation and Version Control › Each PLC program shall be accompanied by a complete set of documentation including a process control narrative, I/O list, tag database export, and full program backups for District record. › PLC program source files shall be maintained under version control. Every program change shall be documented with a revision description, author, date, and reason for change. A known-good backup of the current running program shall be maintained at all times for disaster recovery purposes.	Specification (CRS) establishes the security design standards that must be incorporated into all Operational Technology (OT) projects, including SCADA, Historian, and supporting infrastructure. › CRS requirements are derived from the NIST Cybersecurity Framework (CSF) control objectives and have been integrated into the District's baseline Cybersecurity Policy. › The CRS provides a summarized reference for engineering, integration, and operational teams to ensure consistent implementation of cybersecurity controls across current and future OT projects.	All future SCADA and OT system design, implementation, and integration efforts shall adhere to the CRS and associated District cybersecurity policies.
8.4.8 Testing, Commissioning, and Change Management › All PLC programs shall undergo a structured testing process prior to deployment, including Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT). FAT shall validate logic operation using simulated I/O, and SAT shall verify correct operation with live field devices and instruments. › Test procedures shall document expected results for each test case, including normal operating sequences, alarm conditions, fault responses, failover behavior, and safe-state transitions. Test results shall be recorded and retained as part of the project documentation package.	8.5.2 Key Considerations The general design standards summarized herein do not include the full technical detail contained within the CRS. The CRS provides additional guidance on: › Network segmentation and data flow restrictions to limit access and lateral movement › Access control and role-based permissions for SCADA and supporting systems › System documentation and configuration management practices › Monitoring, logging, alerting, and notification requirements › Backup strategies and system reconstitution procedures › Resource availability to maintain operational continuity › Data security to ensure confidentiality, integrity, and availability	8.5.3 General Cybersecurity Design Standards 8.5.3.1 Security by Design › Security controls shall be considered at system inception and documented as part of all decisions to create, modify, or enhance a SCADA system. › All design documentation shall include the rationale for selected security measures and their expected impact on system operation. 8.5.3.2 Testing and Validation › Test plans shall be established to validate that SCADA systems function as intended, including verification of all security controls, before deployment to production environments. › Updates, patches, and configuration changes shall be tested in a controlled environment to ensure effectiveness and identify potential side effects prior to production implementation. 8.5.3.3 System Hardening and Configuration › Non-essential scripts, services, and software shall be removed or disabled on production systems, except those required for operation or maintenance. › Host-based firewalls shall be installed and enabled on all servers and workstations to restrict access to
8.5 CYBERSECURITY STANDARDS 8.5.1 Overview › The District's Cybersecurity Requirements		

only required services and users.

- › Security controls, including end point protection, software integrity checkers, and web filtering shall be implemented where technically feasible to prevent and detect malware or other threats.
- › Automatic execution of content from removable media shall be disabled.
- › Storage of information shall be limited to authorized locations only.

8.5.3.4 Patch and Vulnerability Management

- › All security patches and firmware updates shall be reviewed, evaluated, and applied in a timely manner following District change management procedures.
- › Software or hardware assets that can no longer be supported, patched, or updated to current versions shall be considered for removal or replacement.

8.5.3.5 Migration and Deployment

- › Migration processes shall be documented and followed to govern the transfer of software and hardware from development to test/staging and then to production environments.
- › Migration procedures shall ensure that security controls are maintained and validated throughout the process.

8.5.3.6 Continuous Security Monitoring

- › SCADA systems shall be periodically reviewed for security compliance, including verification of applied patches, hardening measures, and configuration standards.
- › Any deviations from documented security

controls shall be logged, remediated, and reported to responsible personnel.



9 | PROJECT RECOMMENDATIONS

Projects are divided into three (3) different categories: short-term, mid-term, and long-term. Several mid-term and longer-term term projects are dependent upon completion of one or more short-term projects.

9.1 SHORT-TERM PROJECTS (S)

In general, short-term projects should begin as soon as possible and should be completed within two (2) after the completion of the SCADA Master Plan.

9.1.1 S-1 Radio Communication Infrastructure Upgrade

9.1.1.1 Description

The West Valley Water District (WVWD) currently employs licensed 900 MHz MDS 9710 serial radios to facilitate communication with the majority of its remote sites, operating through a single access point located at the Main Office. The Main Office also maintains links to the Arsenic Treatment Plant via an MDS iNET-II Ethernet radio and to the OPR Water Treatment Plant (WTP) through a Dragonwave point-to-point link. MDS 9710 and iNET-II radios have surpassed their end-of-life (EOL) stage, presenting increasing challenges related to hardware failures, lack of manufacturer support, and unavailability of replacement parts.

This project will implement a modernized radio communication network to replace the

existing legacy infrastructure. The replacement system will utilize licensed 900 MHz GE MDS Orbit radios organized into multiple distributed access point clusters, supported by 5.8 GHz point-to-point Ethernet backbone links between key hub site. The design prioritizes secure, scalable, and resilient communications aligned with the District's broader modernization and cybersecurity strategy. RF path modeling and field survey activities have been conducted to validate the proposed network architecture prior to implementation.

9.1.1.2 Scope

The scope of this project includes the design, procurement, installation, and commissioning of a replacement radio communication network serving approximately 37 remote sites across the District's water system. The project encompasses all activities necessary to replace legacy radio hardware and transition the SCADA communication network to a secure modern, IP-based architecture.

The project will deploy a distributed access point architecture with six access point locations: OPR Water Treatment Plant, Admin/Main Office, Arsenic Treatment Plant, Well 5A, 2-1 Reservoir, and 3-1 Reservoir. Each access point will be equipped with licensed 900 MHz GE MDS Orbit radios, and remote sites will be upgraded from legacy MDS 9710 serial radios to GE MDS Orbit Ethernet radios at mast heights validated through RF modeling and field survey data.

A 5.8 GHz point-to-point Ethernet backbone links will be installed to connect the 2-1 Reservoir access point back to the Admin/Main Office, providing high-bandwidth Ethernet connectivity between hub sites. The existing Dragonwave 23 GHz link between the Admin and OPR sites will be retained. The proposed Well 5A and Arsenic 5.8 GHz backbone paths were evaluated during field surveys and determined to be unsuitable due to tree interference; these sites will communicate via 900 MHz links to the Main Office.

Antenna mast and tower modifications at each access point and remote site will be performed as required to achieve the antenna heights identified in the RF path study. The project will include integration with the existing SCADA communications architecture to ensure all remote telemetry points continue to communicate reliably following cutover. A detailed implementation plan, including site-by-site cutover sequencing, testing procedures, and rollback procedures, will be developed to minimize operational disruption during migration from the legacy system.

The project scope does not include replacement or modification of SCADA host servers, PLCs, or field instrumentation beyond what is necessary to interface with the new radio communication infrastructure.

9.1.1.3 Key Benefits

- › **Elimination of end-of-life radio infrastructure:** Replaces legacy MDS 9710 serial radios that have surpassed

end-of-life, eliminating ongoing risks associated with hardware failures, lack of manufacturer support, and unavailability of replacement parts.

› **Improved communication reliability and network resiliency:** The distributed, multi-access-point architecture eliminates the single-point-of-failure risk inherent in the current single-AP design, ensuring continued SCADA communications to remaining AP clusters if any individual access point becomes unavailable.

› **Transition from serial to IP/Ethernet-based communications:** Replacement with GE MDS Orbit radios provides modern IP/Ethernet-based communication capabilities, enabling higher data throughput, reduced polling cycle durations, and compatibility with modern SCADA and ICS protocols.

› **Enhanced cybersecurity posture:** The new architecture incorporates modern cybersecurity principles, including reduced RF exposure for SCADA telemetry and alignment with the District’s OT security standards, supporting a defense-in-depth communication strategy.

› **Design validated through field survey data:** RF path models were validated through field surveys using GE MDS Orbit radios at proposed antenna heights, confirming reliable signal performance (RSSI generally better than -85 dBm) across all planned 900 MHz radio links prior to implementation.

› **Minimized operational disruption during transition:** Structured site-by-site cutover planning, testing

procedures, and rollback capabilities reduce risk and ensure continuity of SCADA operations during migration from the legacy radio infrastructure.

› **Critical enabler for future PLC modernization:** The District’s future goal of upgrading legacy PLCs to modern controllers is dependent on first transitioning to an Ethernet-based radio network. Legacy serial radios make it extremely challenging to mix different PLC communication protocols across the same network, creating a significant barrier to incremental PLC upgrades. By establishing an Ethernet radio infrastructure, the District will be positioned to transition remote sites from legacy PLCs to modern, IP-capable controllers on a site-by-site basis over time, without requiring a full system cutover and without being constrained by the limitations of serial communication.

9.1.1.4 Assumptions/Prerequisites

The project assumes that the RF path study and field survey results provided by Advanced Integration & Controls (AIC) accurately characterize signal performance under typical operating conditions and that the antenna mast heights identified in the study are structurally feasible at each site. Site access agreements and any required permits for antenna installation and mast modifications are assumed to be obtainable without significant delay.

Licensed spectrum for the 900 MHz radio network is assumed to remain available and that the District’s existing FCC license or a new license can be obtained to support

the expanded network configuration with multiple distributed access points.

The project scope is limited to radio infrastructure replacement and associated antenna, mast, and communications integration work. It does not include replacement or significant modification of SCADA host hardware, field PLCs, or remote instrumentation beyond what is necessary to establish communication over the new radio network.

9.1.1.5 Staffing/Resources

The project requires participation from District personnel with responsibilities in OT operations, SCADA engineering, and field operations to support design reviews, site access coordination, implementation oversight, and system validation activities. District staff will be expected to allocate sufficient time for technical workshops, review of proposed antenna locations and mast heights, coordination of access to remote sites during installation, and participation in site acceptance testing and cutover activities.

9.1.1.5.1 Staffing Requirements

District staff participation will be required for site walkthroughs, hardware installation coordination at remote sites, and final acceptance testing.

9.1.1.5.2 Resource Requirements

The selected consultant/integrator will provide expertise in licensed radio frequency

engineering, GE MDS Orbit radio configuration and deployment, antenna and mast design, point-to-point 5.8 GHz link deployment, and SCADA communication integration, as well as project coordination and technical documentation. Required resources include procurement of licensed 900 MHz GE MDS Orbit radios and associated hardware for all access point and remote site locations, 5.8 GHz point-to-point radio equipment for backbone links, and antenna mast materials as specified in the RF design. Ongoing ownership, monitoring, maintenance, and operational support of the upgraded radio infrastructure will remain the responsibility of the District following project completion.

9.1.1.6 References

- › RF Model Report – WVWD RF Model v1.2 (Advanced Integration & Controls)
- › RF Field Survey Report – AIC WVWD RF Survey Report v1.1 (Advanced Integration & Controls)
- › Cybersecurity Requirements Specification (CRS)
- › FCC License Documentation
- › Cybersecurity Standards
- › Existing SCADA Architecture Diagrams and Network Topology Documentation

9.1.1.7 Estimated Cost

- › \$450,000

9.1.1.8 Estimated Timeframe

- › 20 weeks (NTP to Closeout. Each AP and associated remotes will need to be migrated at same time (one day event).

9.1.2 S-2 HQ System Core Infrastructure Upgrades

9.1.2.1 Description

This project will upgrade and relocate the core compute, storage, and network infrastructure supporting the HQ SCADA system. The objective is to align the HQ architecture with the network segmentation and resiliency standards established at OPR while standardizing on similar hardware platforms to reduce administrative complexity and supportability overhead.

The upgrades will focus on implementing high-availability (HA) firewall, switching, compute, and storage infrastructure to improve system resiliency and operational continuity. The project will also establish a modernized core platform to support the upcoming SCADA system upgrade. Existing SCADA virtual machines (VMs) will be migrated to the new infrastructure, and any necessary modifications to legacy components will be performed to ensure compatibility and continued functionality within the upgraded environment.

9.1.2.2 Scope

The scope of this project includes the design and implementation of a secure, resilient ICS network architecture for the HQ facility in alignment with modern industry best practices and the District’s OT security standards. The compute and storage architecture standards established at OPR will serve as the baseline for the HQ environment. Similarly, firewall and core switching design patterns developed

under the OPR network segmentation and resiliency improvements project will be adopted and extended for HQ implementation.

The project will include comprehensive system design activities, including development of network architecture diagrams, segmentation strategy, firewall zoning and traffic-shaping policies, port assignments, hypervisor and virtualization configurations, and physical network connectivity. These design efforts will be followed by implementation activities to deploy and configure the new infrastructure.

Testing and validation activities will include factory testing, site acceptance testing, and development of a detailed cutover plan to ensure a smooth transition from the legacy infrastructure to the new environment while maintaining existing SCADA application functionality.

The upgraded infrastructure will enable a phased approach to the future SCADA platform upgrade. Given that the new SCADA platform will be a newer version of the existing system from the same manufacturer, the design will consider the integration of legacy SCADA application components into the new platform, allowing them to remain operational until they are individually upgraded. This approach will support operation of both legacy and modernized sites within a unified SCADA application environment.

The overall integration strategy will prioritize maintaining system continuity while enabling incremental upgrades of field systems, PLCs,

and SCADA applications on a site-by-site or grouped basis, in alignment with District standards established through the OPR program.

The project will require careful planning and sequencing of design, infrastructure upgrades, and migration activities to optimize efficiency, minimize cost, and reduce operational disruption.

9.1.2.3 Key Benefits

- › **Improved system resiliency and availability:** Implementation of fully redundant, high-availability (HA) infrastructure for compute, storage, and networking ensures continued operations during hardware failures and supports zero- or near-zero-downtime maintenance.
- › **Alignment with District OT security and architecture standards:** Establishes consistency with the network segmentation and resiliency design patterns developed at OPR, supporting a unified and standardized OT architecture across facilities.
- › **Reduced operational complexity and administrative overhead:** Standardization of hardware platforms and architecture simplifies system management, maintenance, and support activities across HQ and OPR environments.
- › **Enhanced cybersecurity posture:** Incorporates modern ICS security principles, including network segmentation, controlled traffic flows, and secure architecture design aligned with District OT security

policies and requirements.

- › **Foundation for future SCADA platform upgrades:** Provides a modern, scalable infrastructure capable of supporting the next-generation SCADA platform and enabling phased system migration.
- › **Support for phased system modernization:** Enables coexistence of legacy and upgraded SCADA components within a unified environment, allowing incremental upgrades of field systems, PLCs, and SCADA applications without requiring full system replacement.
- › **Minimized operational disruption during transition:** Structured testing, validation, and cutover planning reduce risk and ensure continuity of operations during infrastructure migration.

9.1.2.4 Assumptions/Prerequisites

The project assumes that the architecture standards, hardware selections, and design standards established under the OPR network segmentation and resiliency improvements project are approved by the District for adoption at the HQ facility. It is also assumed that the OPR network segmentation and resiliency improvements project has been completed and is available as a baseline reference for this effort.

The project further assumes that the existing SCADA platform is compatible with the upgraded infrastructure environment, or that any required modifications to ensure compatibility can be performed without significant redesign of application functionality. Planned implementation activities assume the availability of approved maintenance windows to support

infrastructure deployment, system migration, and cutover with minimal operational impact.

Lastly, the project assumes that a suitable location for the new HQ infrastructure has been agreed upon and included as part of the project plan.

The scope is limited to infrastructure upgrades and migration of existing SCADA components and does not include redevelopment of SCADA applications beyond modifications necessary to support operation within the new environment.

9.1.2.5 Staffing/Resources

The project requires participation from District personnel with responsibilities in OT operations, IT infrastructure, network engineering, cybersecurity, and systems engineering to support design, implementation, testing, and migration activities. District staff will be expected to allocate sufficient time for technical workshops, design reviews, system validation, and coordinated cutover activities, including participation during approved maintenance windows.

9.1.2.5.1 Staffing Requirements

The District will provide access to existing infrastructure, system documentation, configuration data, and operational environments necessary to support design and implementation. Required resources include procurement and availability of compute, storage, networking, and firewall hardware, along with associated

software licenses and vendor support contracts to enable high-availability configurations.

9.1.2.5.2 Resource Requirements

The selected consultant/integrator will provide expertise in secure ICS architecture, virtualization, high-availability infrastructure design, network segmentation, and system integration, as well as project coordination and technical documentation. However, ongoing ownership, monitoring, maintenance, and operational support of the upgraded infrastructure will remain the responsibility of the District following project completion.

9.1.2.6 References

- › Cybersecurity Requirements Specification (CRS)
- › Existing Architecture Diagrams
- › Existing Asset Lists
- › Cybersecurity Standards
- › Cybersecurity Requirements Specification (CRS)
- › Hardware Standards
- › HQ Relocation Planning
- › S-4 OPR WFF Network Segmentation & Resiliency Improvements (Prerequisite project)
- › Radio Communication Infrastructure Upgrade
- › Placeholder for project reference to Field, PLC, and SCADA Upgrade Projects (Subsequent projects)

9.1.2.7 Estimated Cost

› \$375,000

9.1.2.8 Estimated Timeframe

- › 32 weeks (NTP to install). Conservative timeframe as lead time for network and server hardware is unstable due to market demand at time of this document.

9.1.3 S-3 HQ SCADA Application Modernization – Wonderware InTouch to AVEVA System Platform Migration

9.1.3.1 Description

This project will modernize the HQ SCADA application by migrating from the legacy Wonderware InTouch platform to AVEVA System Platform, bringing the HQ system into alignment with the AVEVA-based architecture already deployed at the OPR Water Filtration Facility. The migration is designed to support an incremental, site-by-site approach that allows remote sites to be transitioned to System Platform progressively as their associated PLCs and field equipment are upgraded to new hardware, without requiring the District to operate two fully independent SCADA environments in parallel during the transition period.

The core strategy leverages AVEVA System Platform’s ability to host both legacy InTouch WindowViewer components and modern System Platform objects within a unified application environment. This architecture enables a controlled, phased retirement of InTouch-based remote site graphics and I/O configurations as each site completes its PLC and field equipment upgrade,

while maintaining continuous operational visibility across all HQ distribution system sites throughout the transition. The result is a single, unified SCADA application that supports both legacy remote sites and newly upgraded System Platform sites simultaneously, eliminating the operational complexity of running two separate SCADA systems.

9.1.3.2 Scope

The scope of this project includes the design, development, and deployment of a new AVEVA System Platform application for the HQ SCADA system, structured to support the District’s incremental remote site upgrade program. The System Platform application will be architected to serve as the unified SCADA environment for all HQ distribution system sites, enabling coexistence of legacy InTouch-based remote sites and newly upgraded System Platform-based sites within a single application instance during the transition period.

The project will include comprehensive application design activities, including development of the System Platform Galaxy architecture, object model design, I/O server configuration, alarm management strategy, historian integration, and operator display standards aligned with the OPR SCADA implementation. Application design activities will also encompass the InTouch integration architecture, defining how existing InTouch components for legacy remote sites will be hosted within the System Platform environment and the

criteria and workflow for migrating each site as its associated PLC upgrade is completed.

Implementation activities will include deployment of the System Platform server infrastructure, configuration of redundant I/O servers, integration with the Wonderware Historian, migration of the existing HQ SCADA application into the System Platform environment, and development of standardized object templates, graphics, and alarm configurations consistent with the OPR SCADA standard. Operator workstations will be configured to access the System Platform InTouch HMI, providing a unified operator experience.

Testing and validation will include factory acceptance testing (FAT), site acceptance testing (SAT), and development of a detailed cutover plan to ensure a controlled transition from the standalone InTouch system to the System Platform environment, maintaining continuous SCADA coverage of all HQ distribution system sites throughout the migration. The cutover plan will include parallel operation procedures and rollback provisions to minimize operational risk.

Following initial deployment, the project will establish and document the remote site migration workflow – the standardized process by which each remote site is transitioned from InTouch to System Platform as its PLC upgrade is completed. This workflow will define the application engineering activities, testing requirements, and cutover procedures for each incremental site migration,

enabling the District to execute site upgrades independently over time as part of the broader field modernization program.

The project scope does not include PLC upgrades or field device replacements at individual remote sites, which are addressed under separate capital projects. The scope is focused on the SCADA application layer and the associated server infrastructure required to host and operate the new System Platform environment.

9.1.3.3 Key Benefits

- › **Unified SCADA environment across the transition period:** System Platform’s native InTouch integration enables legacy and upgraded remote sites to coexist within a single SCADA application, eliminating the need for the District to operate and maintain separate InTouch and System Platform environments in parallel during the multi-year field upgrade program.
- › **Alignment with the District’s preferred SCADA platform standard:** Establishes HQ on the same AVEVA System Platform architecture deployed at OPR, creating a consistent, standardized SCADA environment across District facilities and reducing the complexity of cross-facility support, training, and system administration.
- › **Incremental remote site upgrade without operational disruption:** Establishes a defined migration workflow that allows each remote site to be transitioned to System Platform on completion of its associated PLC upgrade, enabling the field modernization

program to proceed at a pace determined by budget and operational priorities rather than SCADA system constraints.

- › **Retirement of unsupported and end-of-life SCADA components:** Migrating to System Platform eliminates reliance on the legacy Wonderware InTouch standalone application, which is no longer the District’s preferred platform and presents increasing supportability, cybersecurity, and integration limitations as it ages relative to modern AVEVA software capabilities.
- › **Improved SCADA functionality and operator experience:** System Platform provides a richer application development environment with object-based engineering, enhanced alarm management, improved historian integration, and support for mobile SCADA clients, enabling the District to implement operational improvements that are not available within the legacy InTouch environment.
- › **Foundation for long-term SCADA scalability and integration:** AVEVA System Platform provides a scalable, extensible architecture that supports future integration with third-party data consumers, enterprise reporting solutions, and cloud-based analytics platforms, positioning the District’s SCADA system for long-term operational and technology growth.
- › **Minimized operational disruption during migration:** The phased migration approach, parallel operation provisions, and structured cutover planning ensure that operators maintain continuous SCADA visibility and control of all HQ

distribution system sites throughout the migration, with no requirement for a single large-scale cutover event that would place system availability at risk.

9.1.3.4 Assumptions/Prerequisites

The project assumes that the HQ Core Infrastructure Upgrades project has been completed prior to initiating this effort, providing the modernized compute, storage, and virtualization platform required to host the AVEVA System Platform server environment. It is also assumed that the SCADA Standard Documentation project (S-5) has been completed and that District-approved SCADA application standards, graphic conventions, alarm management guidelines, and object engineering standards are available to guide the System Platform application development.

The project assumes that appropriate AVEVA System Platform, InTouch, and Historian software licenses are procured and available prior to system deployment, and that the selected consultant or integrator has demonstrated experience with AVEVA System Platform application development and InTouch migration projects of comparable scope. It is further assumed that the OPR System Platform application is available as a reference baseline for application architecture, object model design, and graphic standards.

The project assumes that District staff with familiarity with the existing InTouch application, including process narratives, I/O configurations, alarm setpoints, and site-spe-

cific operational requirements, are available to participate in application design reviews and validation activities. Planned implementation activities assume the availability of approved maintenance windows to support system deployment, parallel operation testing, and cutover with minimal operational impact.

The project scope is limited to the SCADA application layer and does not include PLC programming, field device upgrades, or communications infrastructure changes at individual remote sites. PLC and field equipment upgrades are addressed under separate capital projects and serve as the trigger for each incremental remote site migration within the System Platform application.

9.1.3.5 Staffing/Resources

The project requires participation from District personnel with responsibilities in OT operations, SCADA administration, IT infrastructure, and systems engineering to support application design, implementation, testing, and migration activities. District staff will be expected to allocate sufficient time for technical workshops, application design reviews, system validation, operator acceptance testing, and coordinated cutover activities, including participation during approved maintenance windows.

9.1.3.6 Staffing Requirements

District operations staff familiar with current SCADA functionality will be expected to participate in application design reviews, operator acceptance testing, and validation

of migrated site configurations to confirm that the System Platform application meets operational requirements.

9.1.3.7 Resource Requirements

The selected consultant/integrator will provide expertise in AVEVA System Platform application development, InTouch migration, Galaxy architecture design, historian integration, alarm management, and system integration, as well as project coordination and technical documentation. Required resources include procurement and availability of AVEVA System Platform, InTouch HMI, and Historian software licenses sized appropriately for the full HQ tag count and anticipated future growth, along with associated vendor support agreements. Ongoing ownership, administration, and operational support of the System Platform application will remain the responsibility of the District following project completion.

9.1.3.8 References

- › Existing HQ InTouch Application and Configuration Documentation
- › Existing HQ I/O Tag List and Historian Tag Database
- › OPR System Platform Application (Reference Baseline)
- › Cybersecurity Standards
- › Cybersecurity Requirements Specification (CRS)
- › SCADA Software Standards
- › SCADA Standard Documentation
- › HQ System Core Infrastructure

- Upgrades (Prerequisite project)
- › Placeholder for project reference to Remote Site PLC and Field Equipment Upgrade Projects (Subsequent projects, driving incremental site migrations)
- › Process Control Narratives (Blue Books) – Remote Site I/O and Control Documentation

9.1.3.9 Estimated Cost

- › \$200,000

9.1.3.10 Estimated Timeframe

- › Twenty weeks (NTP-Closeout)

9.1.4 S-4 OPR WFF Network Segmentation & Resiliency Improvements

9.1.4.1 Description

This project is intended to align network segmentation and core network resiliency at OPR with current best practices for secure Industrial Control System (ICS) architecture. These practices will establish the District’s standard architecture for the future Headquarters (HQ) system and will be enforced through the District’s OT Security Policy and Cybersecurity Requirements Specification (CRS) developed under the SMP project. Additional network segments will be defined based on the grouping of assets with similar security profiles, functional roles, and access requirements. Existing assets will be reassigned to the appropriate segments, and firewall traffic-shaping and access control policies will be updated accordingly.

The project will also upgrade the firewall and core network switching infrastructure

to fully redundant, active high-availability (HA) configurations. This architecture will enable instantaneous failover and continued operations during degraded conditions resulting from device failures, as well as support zero-downtime maintenance activities, which are not feasible with the current single-firewall and stacked-switch design.

9.1.4.2 Scope

The scope of this project includes the design and implementation of a secure and resilient ICS network architecture at OPR in alignment with modern best practices and District OT security standards. Activities include reviewing the existing network architecture; defining and documenting network segmentation based on asset groupings with similar security profiles, functional roles, and access requirements; and updating the firewall policies with respect to zoning, traffic-shaping, and access control to support the revised segmentation model. The scope further includes reassignment of existing assets to the appropriate network segments and validation of network communications to ensure continued operational functionality.

The project also includes the upgrade of firewall and core network switching infrastructure to fully redundant, active high-availability (HA) configurations to support instantaneous failover, improved resiliency during degraded conditions, and zero-downtime maintenance capabilities. All work will be performed in accordance with the District’s OT Security Policy and Cybersecurity Requirements

Specification (CRS) developed under the SMP project. The scope does not include application-level changes, control system logic modifications, or implementation of new cybersecurity technologies beyond those explicitly defined as part of the network segmentation and core infrastructure upgrades.

The project will require careful planning of activity sequencing to optimize efficiency and minimize cost and operational disruption. The order of network segmentation design, asset reassignment, and resiliency upgrades should be evaluated early in the project to ensure work is not duplicated. Where network infrastructure components are planned for full replacement, network segmentation design and configuration activities should be performed after the hardware upgrades to avoid rework and reduce downtime.

9.1.4.3 Key Benefits

- › **Enhanced Cybersecurity Posture for ICS Environments:** Aligns network segmentation and core infrastructure at OPR with modern secure ICS architecture best practices, reducing the attack surface and limiting lateral movement.
- › **Improved Operational Resilience and Availability:** Implements fully redundant, active high-availability firewall and core switching infrastructure to ensure instantaneous failover, continued operations during degraded conditions, and support for zero-downtime maintenance.
- › **Standardized Architecture for Future Systems:** Establishes a

District-wide reference architecture that will serve as the standard for the future HQ system and other OT environments, enforced through the OT Security Policy and Cybersecurity Requirements Specification (CRS).

- › **Stronger Access Control and Traffic Management:** Enables granular firewall zoning, traffic shaping, and access control based on asset security profiles and operational requirements.
- › **Reduced Risk of Single Points of Failure:** Eliminates reliance on single firewalls and stacked switch configurations, significantly lowering the risk of outages due to hardware failures or maintenance activities.
- › **Improved Compliance and Audit Readiness:** Demonstrates alignment with documented security policies, standards, and industry best practices, supporting regulatory, audit, and internal governance requirements.
- › **Scalable and Maintainable Network Design:** Provides a flexible segmentation model that supports future system expansion, asset onboarding, and evolving security requirements without major architectural redesign.

9.1.4.4 Assumptions/Prerequisites

The project assumes that the District has established OT security standards, including the OT Security Policy and Cybersecurity Requirements Specification (CRS) developed under the SMP project, which will serve as the governing framework for the network design. It is assumed that current network architecture diagrams, asset inventories, IP addressing

schemes, and firewall configurations for OPR are available and sufficiently accurate to support segmentation design and implementation. The District is expected to provide access to relevant OT, IT, and engineering personnel to support design reviews, asset grouping decisions, testing, and implementation activities. Planned implementation activities assume the availability of approved maintenance windows to support asset reassignment, firewall policy updates, and infrastructure upgrades with minimal operational impact. The project further assumes that required hardware, licenses, and support contracts for firewall and core switching upgrades will be procured and available in accordance with the project schedule. Finally, the scope assumes that application configurations, control logic, and vendor-managed systems will not require modification beyond network connectivity changes necessary to support the new segmentation and high-availability architecture.

9.1.4.5 Staffing/Resources

Staffing and resource requirements are essential to ensure that implementation is comprehensive, accurate, and sustainable, supporting the District’s long-term cybersecurity posture and operational continuity.

9.1.4.6 Staffing Requirements

The project requires participation from designated District personnel with responsibility for OT operations, network engineering, cybersecurity, and systems

engineering to support architecture design, asset classification, implementation, and validation activities. District staff are expected to allocate sufficient time to participate in technical workshops, design reviews, testing, and cutover activities, including coordination of approved maintenance windows.

9.1.4.7 Resources Requirements

The District will provide access to current network documentation, asset inventories, configuration information, and operational environments necessary to support implementation. Required resources include procurement and availability of firewall and core switching hardware, licenses, and vendor support contracts to enable active high-availability configurations. The consultant will provide specialized expertise in secure ICS network architecture, segmentation design, high-availability implementation, and technical documentation; however, ongoing operational support, monitoring, and maintenance of the upgraded network infrastructure will remain the responsibility of the District following project completion

9.1.4.8 References

- › Cybersecurity Requirements Specification (CRS)
- › Existing Architecture Diagrams
- › Existing Asset Lists
- › Cybersecurity Standards
- › Cybersecurity Requirements Specification (CRS)

9.1.4.9 Estimated Cost

› \$85,000

9.1.4.10 Estimated Timeframe

› Fourteen weeks (NTP-Closeout)

9.1.5 S-5 PLC Standard Documentation

9.1.5.1 Description

This project is intended to develop formal PLC standard documentation that captures the programming and tag standards developed and implemented for the OPR system. While the District has identified the OPR PLC programming and tag conventions as the baseline standard for future PLC development, these standards are not currently documented in a formal District PLC programming standards document. This project will produce a comprehensive and authoritative PLC programming standard to formally codify these practices. The resulting standard will serve as a reference for future District PLC development efforts and will be leveraged by the Headquarters (HQ) PLC upgrade project to support consistent design, integration, and implementation.

9.1.5.2 Scope

The scope of this project includes the development of a formal District PLC programming standards document based on the programming, tag naming, and structural conventions implemented in the OPR system. Activities include reviewing existing OPR PLC programs, configurations, and supporting documentation; identifying and documenting standard

programming practices, tag structures, naming conventions, and organizational methodologies; and validating the documented standards with District stakeholders. The project will produce a comprehensive PLC standards document intended to serve as the District’s authoritative reference for future PLC development and upgrades. The scope further includes formatting, review, and finalization of the standard to support adoption by the HQ PLC upgrade project. The scope does not include modification of existing PLC logic, development of new PLC programs, or implementation activities beyond documentation and stakeholder validation.

9.1.5.3 Key Benefits

- › **Establishment of a Formal District PLC Programming Standard:** Codifies the PLC programming and tag standards implemented in the OPR system into an authoritative, documented standard for District-wide use.
- › **Consistency Across Current and Future PLC Implementations:** Ensures uniform programming practices, tag naming, and structural conventions across projects, reducing variability and integration risk.
- › **Improved Efficiency in Future PLC Design and Integration:** Provides clear guidance that accelerates PLC development, review, and integration activities, particularly for the HQ PLC upgrade project.
- › **Reduced Risk of Configuration Errors and Rework:** Standardized programming practices improve code readability, maintainability, and reliability, lowering the likelihood

of defects and misinterpretation.

- › **Enhanced Maintainability and Knowledge Transfer:** Improves long-term system support by enabling easier troubleshooting, onboarding of new staff and integrators, and preservation of institutional knowledge.
- › **Support for Governance And Quality Assurance:** Enables consistent application of District engineering standards and facilitates code reviews, acceptance testing, and vendor oversight.
- › **Foundation for Scalable and Sustainable OT Operations:** Establishes a repeatable framework that supports future system expansion, upgrades, and modernization efforts.

9.1.5.4 Assumptions/Prerequisites

This project should be executed concurrently with the SCADA Standards Documentation project due to the direct relationship and interdependencies between PLC programming and tag standards and the corresponding SCADA application programming and tag structures.

The project assumes that the OPR system PLC programs, tag databases, and related documentation are available and accessible for review and analysis. It is assumed that the District has identified and approved the OPR PLC programming and tag conventions as the acceptable baseline standard for future PLC development and that key District stakeholders will be available to participate in reviews and validation of the documented standards. The project further assumes that the effort is limited to documentation and standardization of existing practices

and does not include modification, refactoring, or redevelopment of PLC logic. The resulting PLC standards document is intended to be used as guidance for future projects, including the HQ PLC upgrade, and its adoption and enforcement will be managed through District governance and project oversight processes.

9.1.5.5 Staffing/Resources

Staffing and resource requirements are essential to ensure that standards documentation is comprehensive, accurate, and sustainable, supporting the District’s long-term standards and operational continuity.

9.1.5.6 Staffing Requirements

The project requires participation from District personnel with expertise in PLC programming, controls engineering, and OT operations to support review of existing OPR PLC programs and validation of documented standards. District staff are expected to allocate time for interviews, workshops, and document reviews to confirm programming practices, tag conventions, and design intent.

9.1.5.7 Resource Requirements

The District will provide access to relevant PLC source code, tag databases, system documentation, and development environments as needed to support analysis and documentation. The consultant will provide subject matter expertise in PLC standards development, facilitate stakeholder coordination, and produce the formal PLC standards document; however, ongoing

ownership, maintenance, and enforcement of the standard will remain the responsibility of the District following project completion.

9.1.5.8 References

- › Existing OPR WFF PLC Programs
- › Software Documentation Standards
- › S-5 SCADA Standard Documentation (Concurrent project)

9.1.5.9 Estimated Cost

› \$50,000

9.1.5.10 Estimated Timeframe

› Eight weeks (NTP-Closeout)

9.1.6 S-6 SCADA Standard Documentation

9.1.6.1 Description

This project is intended to develop formal SCADA application programming standards documentation that captures the practices developed and implemented for the OPR system, including standards for graphics, application logic, alarming, historical data, and tag structures. While the District has identified the OPR SCADA application programming as the baseline standard for future SCADA development, these practices are not currently documented in a formal District SCADA application programming standards document. This project will produce a comprehensive and authoritative SCADA application programming standard to formally codify these practices. The resulting standard will serve as a reference for future District SCADA development efforts

and will be leveraged by the Headquarters (HQ) SCADA upgrade project to support consistent design, integration, and implementation.

9.1.6.2 Scope

The scope of this project includes the development of a formal District SCADA application programming standards document based on the application programming practices implemented in the OPR system. Activities include reviewing existing OPR SCADA applications, tag structures, naming conventions, configurations, and supporting documentation; identifying and documenting standards for graphics development, application logic, alarming, historical data collection, tag naming and structure, and overall application organization; and validating the documented standards with District stakeholders. The project will produce a comprehensive and authoritative SCADA application programming standards document intended to serve as the District’s reference for future SCADA development and modernization efforts. The scope further includes formatting, review, and finalization of the standards documentation to support adoption by the HQ SCADA upgrade project. The scope does not include modification of existing SCADA applications, development of new application functionality, or system implementation activities beyond documentation and stakeholder validation.

9.1.6.3 Key Benefits

- › **Establishment of a Formal District SCADA Application Programming Standard:** Codifies the SCADA application

- programming and tag standards implemented in the OPR system into an authoritative, documented standard for District-wide use.
- › **Consistency Across Current and Future PLC Implementations:** Ensures uniform standards for graphics, logic, alarming, historical data, and tag structures, reducing variability and integration risk across projects.
 - › **Improved Efficiency in Future SCADA Design and Integration:** Provides clear guidance that accelerates application development, configuration, and review activities, particularly for the HQ SCADA upgrade project.
 - › **Reduced Risk of Configuration Errors and Rework:** Standardized programming practices improve application quality, maintainability, and reliability, lowering the likelihood of defects and misinterpretation.
 - › **Enhanced Maintainability and Knowledge Transfer:** Improves long-term system support by enabling easier troubleshooting, onboarding of new staff and integrators, and preservation of institutional knowledge.
 - › **Support for Governance and Quality Assurance:** Enables consistent application of District engineering standards and facilitates code reviews, acceptance testing, and vendor oversight.
 - › **Foundation for Scalable and Sustainable OT Operations:** Establishes a repeatable framework that supports future system expansion, upgrades, and modernization efforts.

9.1.6.4 Assumptions/Prerequisites

This project should be executed concurrently with the PLC Standards Documentation project due to the direct relationship and interdependencies between PLC programming and tag standards and the corresponding SCADA application programming and tag structures.

The project assumes that the OPR SCADA system applications, configurations, tag databases, graphics libraries, alarming configurations, and historical data setups are available and accessible for review. It is assumed that the District has identified and approved the OPR SCADA application programming practices as the acceptable baseline standard for future SCADA development and that relevant District stakeholders will be available to participate in interviews, reviews, and validation of the documented standards. The effort is limited to documentation and formalization of existing practices and does not include modification, refactoring, or redevelopment of SCADA applications. Adoption, enforcement, and ongoing maintenance of the resulting SCADA application programming standards will be managed through District governance and project oversight processes. The standards are intended to inform and support future initiatives, including the HQ SCADA upgrade project.

9.1.6.5 Staffing/Resources

Staffing and resource requirements are essential to ensure that standards documentation is comprehensive, accurate, and sustainable, supporting the District's long-term standards and operational continuity.

- 9.1.6.6 Staffing Requirements
- The project requires participation from District personnel with expertise in SCADA application development, OT operations, controls engineering, and system administration to support review of existing OPR SCADA applications and validation of documented standards. District staff are expected to allocate time for interviews, workshops, and document reviews to confirm application design practices, configuration conventions, and operational intent.
- 9.1.6.7 Resource Requirements
- The District will provide access to relevant SCADA development environments, application files, configuration data, and supporting documentation necessary to support analysis and documentation. The consultant will provide subject matter expertise in SCADA standards development, facilitate stakeholder coordination, and produce the formal SCADA application programming standards document; however, ongoing ownership, maintenance, and enforcement of the standard will remain the responsibility of the District following project completion.
- 9.1.6.8 References
- › Existing OPR WFF SCADA Application
 - › Software Documentation Standards
 - › S-4 PLC Standard Documentation (Concurrent project)
- 9.1.6.9 Estimated Cost
- › \$60,000

- 9.1.6.10 Estimated Timeframe
- › Eight weeks (NTP-Closeout)
- 9.2 MID-TERM PROJECTS (M)
- Mid-term projects typically begin within two (2) years after completion of the SCADA Master Plan and are often several years in duration but should be completed within five (5) years after the completion of the SCADA Master Plan.
- 9.2.1 M-1 Cybersecurity Control Gap (Re)Assessment
- 9.2.1.1 Description
- This project is intended to re-assess the District's cybersecurity controls following the integration of baseline policies, the Incident Response and Recovery Plan, and other changes that may have affected the District's overall cybersecurity posture. Related initiatives, including projects such as the OPR network segmentation and resiliency improvements, are expected to influence cybersecurity control effectiveness and will be considered as part of the reassessment.
- The project will also establish a defined cadence and methodology for future cybersecurity control reassessments to ensure the District's cybersecurity posture is evaluated on a regular basis as systems, technologies, organizational structures, and industry best practices evolve over time.
- 9.2.1.2 Scope

The scope of this project includes a comprehensive reassessment of the District's cybersecurity controls to evaluate their effectiveness following the implementation of baseline cybersecurity policies, the Incident Response and Recovery Plan, and other completed or in-progress initiatives that may impact the District's cybersecurity posture. Activities include reviewing existing administrative, technical, and operational controls; assessing alignment with current cybersecurity standards, industry best practices, and District requirements; and evaluating the impact of related projects, such as network segmentation and resiliency improvements, on overall control effectiveness.

The project will document current-state cybersecurity control maturity, identify gaps and improvement opportunities, and provide prioritized recommendations to address identified risks. The scope further includes establishing a defined methodology and recommended frequency for future cybersecurity control reassessments to support ongoing governance, continuous improvement, and long-term cybersecurity resilience. The scope does not include implementation of new cybersecurity controls or technologies unless explicitly defined in a separate engagement.

9.2.1.3 Key Benefits

- › **Validated Effectiveness of Cybersecurity Controls:** Provides an updated, objective assessment of the District's cybersecurity controls following recent policy, incident response, and system changes.

- › **Improved Risk Visibility and Prioritization:** Identifies gaps, control weaknesses, and residual risks, enabling informed prioritization of remediation efforts and resource allocation.
 - › **Alignment with Evolving Standards and Best Practices:** Ensures cybersecurity controls remain aligned with current industry standards, regulatory expectations, and ICS cybersecurity best practices.
 - › **Integration of Related Security Initiatives:** Evaluates the cumulative impact of related projects, such as network segmentation and resiliency improvements, on the District's overall cybersecurity posture.
 - › **Support for Governance, Compliance, and Audit Readiness:** Produces documented assessment results and recommendations that support internal governance, external audits, and regulatory inquiries.
 - › **Foundation for Continuous Improvement:** Establishes a repeatable reassessment methodology and cadence, enabling the District to systematically evaluate and improve its cybersecurity posture over time.
 - › **Informed Decision-Making for Future Investments:** Provides actionable insights that support strategic planning and future cybersecurity technology and control investments.
- 9.2.1.4 Assumptions/Prerequisites
- The project assumes that the District's baseline cybersecurity policies, Incident Response and Recovery Plan, and related governance

documentation have been finalized and are available for review. It is assumed that sufficient documentation and evidence of existing administrative, technical, and operational cybersecurity controls can be provided, including policies, procedures, system configurations, and prior assessment materials. The District will make available appropriate OT, IT, cybersecurity, and management personnel to support interviews, walkthroughs, and validation activities. The assessment further assumes that information regarding related initiatives, such as network segmentation and resiliency improvement projects, will be available to evaluate their impact on the District's cybersecurity posture. The scope of this effort is limited to assessment and recommendations and does not include implementation of new controls or remediation activities unless explicitly defined in a separate scope.

9.2.1.5 Staffing/Resources

Staffing and resource requirements are essential to ensure that the security controls assessment is comprehensive, accurate, and sustainable, supporting the District's long-term cybersecurity posture and operational continuity.

9.2.1.6 Staffing Requirements

The project requires participation from District personnel with responsibilities in cybersecurity, OT operations, IT, engineering, and management to support interviews, evidence collection, and validation of cybersecurity

controls. District staff are expected to allocate sufficient time to participate in assessment activities, including document reviews, technical walkthroughs, and stakeholder meetings.

9.2.1.7 Resource Requirements

The District will provide access to relevant cybersecurity policies, procedures, system configurations, prior assessment results, and supporting evidence necessary to conduct the reassessment. The consultant will provide cybersecurity assessment expertise, facilitation, analysis, and reporting; however, ownership of cybersecurity controls, ongoing monitoring, and implementation of any recommended improvements will remain the responsibility of the District following completion of the assessment.

9.2.1.8 References

- › SCADA Cybersecurity Assessment Report
- › Security Controls Gap Assessment
- › Baseline Security Policy Integration
- › Response and Recovery Plan Integration
- › S-4 OPR WFF Network Segmentation & Resiliency Improvements (Prerequisite project)

9.2.1.9 Estimated Cost

- › \$48,000

9.2.1.10 Estimated Timeframe

- › Eight weeks (NTP-Closeout)

9.2.2 M-2 Response and Recovery Plan Integration

9.2.2.1 Description

This project is intended to integrate the District's SCADA Incident Response and Recovery Plan (IRRP), developed under the SMP project, into applicable Operational Technology (OT) and business practices and procedures. Integration will be achieved through collaboration with relevant District departments and stakeholders to ensure that plan integration, role assignments, training, and operational procedures takes place and is properly aligned with the established organizational structure. The IRRP will be tailored to the District's operational context to ensure it is practical, enforceable, and consistent with organizational objectives.

9.2.2.2 Scope

The implementation scope includes reviewing the existing SCADA Incident Response and Recovery Plan (IRRP) developed under the SMP project to assess its applicability to current District operations along with the baseline security policy related to response and recovery; collaborating with relevant District departments and stakeholders to define incident response and recovery roles, responsibilities, and decision-making authority; aligning IRRP procedures with existing OT operations, business processes, and governance frameworks; tailoring the IRRP to reflect the District's operational environment, systems, staffing model, and risk profile; developing or updating supporting procedures, workflows, and documentation required for effective implementation; identifying training needs

and supporting the development of role-based training and awareness activities; facilitating tabletop exercises or walkthroughs, as appropriate, to validate plan integration and operational readiness; and establishing mechanisms for ongoing maintenance, periodic review, and continuous improvement of the IRRP.

9.2.2.3 Key Benefits

- › **Operational Resilience and Continuity:** Strengthens the District's ability to rapidly detect, respond to, and recover from SCADA and OT incidents, minimizing service disruption and operational impact.
- › **Clear Governance and Decision Authority:** Establishes unambiguous roles, responsibilities, and escalation pathways, enabling timely and coordinated decision-making during high-impact incidents.
- › **Risk Reduction Tailored to the District Environment:** Aligns incident response and recovery procedures to the District's specific operational context, systems, staffing model, and risk profile, improving effectiveness and relevance.
- › **Improved Cross-Functional Coordination:** Enhances alignment between OT operations, IT, cybersecurity, and business stakeholders, reducing response friction and improving overall incident management.
- › **Regulatory, Audit, and Compliance Support:** Provides documented, tested, and repeatable processes that support regulatory expectations, audit requirements, and industry best practices for critical infrastructure protection.

- › **Workforce Readiness and Capability Building:** Increases staff preparedness through role-based training and exercises, ensuring personnel understand their responsibilities before an incident occurs.
- › **Validated and Continuously Improving Response Capability:** Uses exercises, reviews, and maintenance processes to identify gaps, incorporate lessons learned, and continuously strengthen the IRRP over time.

9.2.2.4 Assumptions/Prerequisites

The engagement assumes that the District has completed the Baseline Security Policy Integration project and that an existing SCADA Incident Response and Recovery Plan, both developed under the SMP project, is available for review and update, and that District leadership will provide active sponsorship and timely decision-making support. It is assumed that relevant District departments and stakeholders, including OT operations, IT, cybersecurity, legal, communications, and emergency management, will participate as needed in planning, review, training, and validation activities. The District is expected to provide access to current and reasonably accurate documentation related to OT and SCADA systems, architectures, inventories, governance frameworks, and operational processes to support plan alignment and tailoring. Personnel assigned incident response and recovery roles are assumed to be available to support interviews, training, and tabletop exercises, which will be conducted using existing District facilities and tools unless

otherwise agreed. The engagement further assumes that implementation activities are limited to planning, documentation, training, and exercises, and do not include the deployment of new technical controls or system upgrades unless explicitly defined in a separate scope.

9.2.2.5 Staffing/Resources

Staffing and resource requirements are essential to ensure that IRR plan integration is comprehensive, accurate, and sustainable, supporting the District's long-term cybersecurity posture and operational continuity.

9.2.2.6 Staffing Requirements

The engagement requires participation from designated District personnel with operational, technical, and governance responsibilities related to SCADA and OT environments. This includes representation from OT operations, IT, cybersecurity, engineering, emergency management, legal, communications, and executive leadership to support planning, review, decision-making, and validation activities. Engagement also includes coordination with appropriate designated third party and external support resources including management of SLAs, NDAs, and other relevant agreements as defined and implemented in District policy. District staff are expected to allocate sufficient time to participate in workshops, interviews, document reviews, training sessions, and tabletop exercises.

9.2.2.7 Resource Requirements

The District will provide access to relevant facilities, systems documentation, policies, and collaboration tools necessary to support the engagement. The consultant will provide subject matter expertise, facilitation, documentation development, and coordination support; however, ongoing operational ownership, staffing, and resourcing for incident response and recovery activities will remain the responsibility of the District following implementation.

9.2.2.8 References

- › SCADA Incident Response and Recovery Plan
- › Response and Recovery Plan

9.2.2.9 Estimated Cost

- › \$40,000

9.2.2.10 Estimated Timeframe

- › Eight weeks (NTP-Closeout)

9.3 LONG-TERM PROJECTS (L)

Longer-term projects typically occur in the three (3) to six (6) year timeframe after completion of the SCADA Master Plan and should be completed within ten (10) years after the completion of SCADA Master Plan.

9.3.1 L-1 Remote Site Panel, PLC, and SCADA Upgrade Program

9.3.1.1 Description

This project will execute a comprehensive upgrade program for remote site control panels, programmable logic controllers (PLCs), PLC programming, and associated SCADA ap-

plication modifications across the District’s HQ distribution system. The objective is to replace the legacy Tesco LIQ PLCs and aging field control panel infrastructure at approximately 37 remote sites with modern, industry-standard Allen-Bradley CompactLogix controllers installed in new or retrofit control panel enclosures, standardize PLC programming in accordance with District PLC programming standards, and integrate each upgraded site into the AVEVA System Platform SCADA application.

The HQ distribution system currently relies on proprietary Tesco LIQ PLCs across multiple generations, creating single-source vendor dependency, inconsistent hardware capabilities, and significant long-term supportability and supply chain risk. Field control panels at the majority of remote sites exhibit aging infrastructure dating from the late 1980s through the early 2000s, including degraded enclosures, lack of proper voltage separation, absence of surge protection and cooling, and insufficient cybersecurity provisions. These conditions have been documented through the comprehensive system assessment conducted as part of the SCADA Master Plan.

Given the large number of remote sites requiring upgrades, this project is structured as a multi-phase program spanning both mid-term and long-term planning horizons. The District should prioritize which sites fall under the mid-term phase based on the findings of the system assessment report, considering factors such as equipment condition, criticality to system

operations, safety risk, and cybersecurity exposure. The remaining lower-priority remote sites will be categorized under the long-term project phase. This phased approach allows the District to allocate capital resources strategically while maintaining continuous system operations throughout the upgrade program.

Each site upgrade will include replacement of the existing PLC with an Allen-Bradley CompactLogix controller and associated I/O modules, development of standardized PLC programming using District-approved Add-On Instructions (AOIs) and tag naming conventions, panel enclosure replacement or refurbishment to meet current UL508A, District standards, and SCADA application modifications to migrate the site from the legacy InTouch to AVEVA System Platform. The typical panel design and bill of materials documented in Companion Document K will serve as the baseline standard for all remote site panel upgrades.

9.3.1.2 Scope

The scope of this project encompasses the design, engineering, procurement, installation, programming, testing, and commissioning of upgraded remote site control panels, PLCs, and SCADA integration for all HQ distribution system remote sites. Priority sites can be moved into mid-term phase if schedule and budget permits:

Mid-Term Phase (Priority Sites): The mid-term phase will address remote sites identified

as highest priority based on the system assessment report. Prioritization criteria include severity of existing panel and PLC deficiencies, criticality of the site to District water system operations, safety and code compliance risk factors, cybersecurity exposure, and current operational limitations such as sites operating only in hand control mode. The mid-term phase should begin within two years after completion of the SCADA Master Plan and be completed within five years.

Long-Term Phase (Remaining Sites): The long-term phase will address the remaining remote sites not included in the mid-term phase. These sites, while still requiring modernization, present lower immediate risk or operational impact relative to the priority sites. The long-term phase should begin within three to four years after completion of the SCADA Master Plan and be completed within ten years.

Site-Level Scope of Work: For each remote site, the scope of work includes:

- › Removal and replacement of the existing Tesco LIQ PLC with an Allen-Bradley CompactLogix controller and associated I/O modules sized to accommodate existing and anticipated future I/O requirements
- › Development and deployment of standardized PLC programming utilizing District-approved Add-On Instructions (AOIs) for motor control, valve control, analog instrument processing, alarm logic, and PID control, in accordance with the PLC Programming Standards document

- › Redesign of PLC alarm logic to eliminate common or grouped alarms and implement specific, actionable, and prioritized alarm points with appropriate on-delay timers, deadbands, and alarm suppression or dependency logic
- › Expansion of PLC-to-SCADA diagnostic data to include PLC processor health, I/O module fault status, communication link status, intrusion detection status, and equipment runtime counters
- › Replacement of legacy serial communication protocols with industry-standard industrial Ethernet protocols (EtherNet/IP) to support modern SCADA integration over the upgraded radio communication network
- › Panel enclosure replacement or retrofit in accordance with the typical panel design documented in Companion Document K, including proper voltage separation, UL508A compliance, surge protection, cooling provisions, enclosure lighting, intrusion switches, and managed Ethernet switches
- › Rewiring and reconnection of field instrumentation, motor control interfaces, and power distribution within the upgraded panel, including proper labeling and documentation of all wire terminations
- › Integration of upgraded PLC into the AVEVA System Platform SCADA application, including development of standardized System Platform objects, graphics, alarm configurations, and historian tags for the site, replacing the legacy InTouch-based SCADA components

- › Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) for each upgraded site, including verification of all PLC I/O, process control logic, alarm functionality, SCADA communications, and operator display accuracy
- › Development of site-specific cutover plans to ensure controlled transition from legacy to upgraded systems with minimal operational disruption, including rollback provisions
- › Update of process control narrative documentation to reflect the upgraded PLC programming and control logic for each site

The project scope does not include major civil, structural, or mechanical modifications at remote sites beyond what is necessary to install the upgraded control panels or backpans. It also does not include replacement of field instrumentation or motor control equipment unless such equipment is found to be incompatible with the upgraded PLC platform and cannot be reasonably interfaced.

9.3.1.3 Key Benefits

- › **Elimination of proprietary, single-source PLC vendor dependency:** Replaces legacy Tesco LIQ PLCs with industry-standard Allen-Bradley CompactLogix controllers, eliminating the single-source vendor dependency for hardware, replacement parts, firmware support, and programming services that currently presents significant long-term supportability and supply chain risk.
- › **Standardization of PLC hardware and programming across all District**

facilities: Aligns all HQ distribution system remote sites with the Allen-Bradley platform and PLC programming standards established at OPR, enabling consistent hardware, programming tools, spare parts inventories, and staff training across the District.

- › **Improved field panel safety, code compliance, and reliability:** Addresses critical field panel deficiencies identified in the system assessment, including proper voltage separation, UL508A short circuit current rating validation, surge protection, cooling, and enclosure integrity, bringing remote site panels into compliance with current safety codes and reliability standards.
- › **Enhanced cybersecurity posture at remote sites:** Incorporates standardized PLC-monitored physical and logical security at each site, including intrusion detection for electrical panels and site access, unique PLC program passwords, managed Ethernet switches, and consistent access control practices aligned with District OT security standards.
- › **Improved alarm quality and operational visibility:** Redesigned PLC alarm logic eliminates common or grouped alarms and implements specific, actionable, and prioritized alarm points, improving fault identification and reducing nuisance alarms. Expanded PLC-to-SCADA diagnostic data provides operators with proactive visibility into controller and field device health.
- › **Unified SCADA application environment:** Each upgraded site is migrated from the legacy InTouch

environment to AVEVA System Platform, progressively building toward a single, unified SCADA application that supports both legacy and upgraded sites during the transition and eliminates reliance on the legacy InTouch standalone application.

- › **Foundation for long-term system sustainability and District self-reliance:** Standardized PLC programming using well-documented, reusable function blocks and comprehensive inline documentation enables qualified District staff to maintain and troubleshoot the system without external integrator dependency for routine tasks.

9.3.1.4 Assumptions/Prerequisites

This project assumes that several prerequisite projects identified in the SCADA Master Plan have been completed or are sufficiently advanced prior to initiating remote site upgrades. Specifically, the Radio Communication Infrastructure Upgrade (S-1) must be completed to provide the Ethernet-based radio communication network required to support the modern Allen-Bradley PLCs at remote sites. The HQ System Core Infrastructure Upgrades (S-2) and HQ SCADA Application Modernization (S-3) must be completed to provide the infrastructure and AVEVA System Platform application environment into which upgraded remote sites will be integrated. The PLC Standard Documentation (S-5) and SCADA Standard Documentation (S-6) projects must be completed to provide the formal programming and application standards that will govern PLC development and SCADA integration for each site.

The project assumes that the system assessment report, including site-by-site field assessment findings documented as part of the SCADA Master Plan, is available and will serve as the basis for prioritization of mid-term versus long-term site upgrades. The District is expected to review the assessment findings and approve the site prioritization and phasing prior to the start of design activities for each phase.

The project further assumes that the typical panel design and bill of materials documented in Companion Document K are approved by the District as the baseline standard for remote site panel upgrades. Site-specific design variations may be required to accommodate unique physical constraints, I/O configurations, or operational requirements at individual sites, but the Companion Document K design will serve as the standard starting point.

It is assumed that the existing process control narratives (blue books) and the consolidated remote site I/O and control documentation are available and sufficiently accurate to support PLC programming development. Any discrepancies between documented and actual field conditions will be identified and resolved during the design and FAT phases.

Planned implementation activities assume the availability of approved maintenance windows at each site to support panel installation, PLC cutover, and SCADA integration with minimal operational disruption. The project assumes that site access and coordination

requirements can be managed within normal project scheduling without significant delays.

The scope is limited to PLC, control panel, PLC programming, and SCADA application modifications at remote sites and does not include upgrades to the core SCADA infrastructure, radio communication network, or SCADA server environment, which are addressed under separate prerequisite projects.

9.3.1.5 Staffing/Resources

District operations and maintenance staff familiar with individual remote site operations, process control requirements, and field equipment will be expected to participate in site-specific design reviews, FAT/SAT activities, and cutover operations. District SCADA and controls engineering staff will participate in PLC programming standard reviews, SCADA application design reviews, and system validation to confirm that upgraded sites meet operational and cybersecurity requirements.

9.3.1.6 Resource Requirements

The selected consultant/integrator will provide expertise in Allen-Bradley CompactLogix PLC programming, AVEVA System Platform application development, control panel design and fabrication, field installation and commissioning, and SCADA system integration, as well as project coordination and technical documentation. Required resources include procurement and availability of Allen-Bradley CompactLogix controllers, I/O modules, power supplies, managed Ethernet switches, panel

enclosure materials, and associated hardware for each site upgrade, consistent with the Companion Document K typical panel design and site-specific I/O requirements. AVEVA System Platform software licensing must be sized to accommodate the incremental tag count growth as sites are migrated. Ongoing ownership, monitoring, maintenance, and operational support of the upgraded PLCs, control panels, and SCADA application components will remain the responsibility of the District following project completion.

9.3.1.7 References

- › SCADA Master Plan – System Assessment Report and Site-by-Site Field Assessment Findings
- › SCADA Master Plan – Companion Document K: Typical Panel Design and Bill of Materials
- › Process Control Narratives (Blue Books) – Remote Site I/O and Control Documentation
- › PLC Programming Standards Document (S-5)
- › SCADA Application Programming Standards Document (S-6)
- › Cybersecurity Requirements Specification (CRS)
- › Cybersecurity Standards
- › Hardware Standards
- › Existing Architecture Diagrams and Asset Lists
- › S-1 Radio Communication Infrastructure Upgrade (Prerequisite project)

- › S-2 HQ System Core Infrastructure Upgrades (Prerequisite project)
- › S-3 HQ SCADA Application Modernization (Prerequisite project)
- › S-5 PLC Standard Documentation (Prerequisite project)
- › S-6 SCADA Standard Documentation (Prerequisite project)

9.3.1.8 Estimated Cost

- › \$4,630,000

9.3.1.9 Estimated Timeframe

- › 45 weeks (NTP-Closeout)

10^{COMPANION} DOCUMENTS

The following companion documents were developed as part of the West Valley Water District SCADA Master Plan. These documents are maintained separately from the Master Plan because they are intended to serve as living documents that support ongoing District operations.

Ownership of these documents transfers to the District upon project completion. As systems, policies, standards, and operational requirements evolve, each document should be reviewed and updated to reflect current conditions.

- A Networks & Assets
- B System Architecture
- C RF System and Proposed Model
- D Process Control Narratives
- E Configuration Summaries
- F Cybersecurity Gap Assessment
- G Wireless Backhaul and RF Telemetry System
- H Cybersecurity Requirements Summary
- I Response and Recovery Plan
- J Baseline Policies and Procedures
- K Typical Drawings and Bill of Materials
- L Recommended Project Schedule
- M Needs Assessment Matrix





STAFF REPORT

DATE: September 15, 2026

TO: Safety and Technology Committee

FROM: Jon Stephenson, Director of Technical Services

SUBJECT: Professional Services Agreement with SDI Presence, LLC for an IT Master Plan

STRATEGIC GOAL:

Strategic Goal 1 - Manage and Deliver a Safe, Reliable, and Sustainable Water Supply; Objective 1E. Ensure Operational Continuity through Comprehensive Physical and Cyber Security

Strategic Goal 5 – Apply Sound Planning, Innovation, and Best Practices; Objective 5A. Increase Operational Efficiency, Resiliency, and Reliability

MEETING HISTORY:

N/A.

BACKGROUND:

It is best practice to prepare an Information Technology ("IT") Master Plan every five (5) years to align an organization's technology capabilities with its broader business goals as outlined in the Strategic Plan.

DISCUSSION:

West Valley Water District, ("District"), has not previously developed or adopted a formal IT Master Plan. Staff issued a Request for Proposal ("RFP") to prepare a comprehensive IT Master Plan for the current and future District needs. This RFP was posted on PlanetBids. The District received proposals from seven (7) Consulting firms: Avero Advisors; BerryDunn; BuzzClan, LLC; SDI Presence, LLC; Solutionz, Inc; The OMNI Group, LLC; and Timmons Group. The seven (7) proposals received included similar qualifications and technical expertise.

To determine the best value for the District, staff ensured that all proposals received met the minimum requirements in the scope of work. Staff evaluated and scored the received proposals based on the scoring criteria described in the RFP and SDI Presence, LLC was the highest rated proposal. Attached as Exhibit A is the standard District Professional Services Agreement with SDI Presence, LLC which includes the negotiated scope of work.

This item is in support of the District's Strategic Plan Goal for managing and delivering a safe, reliable, and sustainable water supply by ensuring operational continuity through comprehensive physical and cyber security, as well as the District's Strategic Plan Goal of applying sound planning, innovation, and best practices to increase operation efficiency, resiliency, and reliability.

FISCAL IMPACT:

The cost to perform the services for the development of the IT Master Plan as proposed by SDI Presence, LLC is \$115,960.00. This item is included in the Fiscal Year 2026/27 Department Budget under GL Account 100-5640-525-5316 for \$150,000.

REQUESTED ACTION:

Staff recommends that the Committee forward a recommendation to the Board of Directors to:

1. Approve a Professional Services Agreement and Task Order No. 1 with SDI Presence, LLC in the amount of \$115,960.00 for IT Master Planning Services and;
2. Authorize the General Manager to execute all necessary documents.

Attachments

[Attachment A - Professional Services Agreement SDI Presence, LLC 9.2.2026.pdf](#)

ATTACHMENT A

PROFESSIONAL SERVICES AGREEMENT – SDI PRESENCE, LLC



West Valley Water District

AGREEMENT FOR PROFESSIONAL SERVICES

With

SDI Presence, LLC

TABLE OF CONTENTS

	Page
Section 1. Term of Agreement.....	1
Section 2. Scope and Performance of Services.	1
Section 3. Additional Services and Changes in Services.....	3
Section 4. Familiarity with Services and Site.	3
Section 5. Compensation and Payment.....	4
Section 6. Required Documentation Prior to Performance.	5
Section 7. Project Documents.	5
Section 8. Consultant's Books and Records.....	5
Section 9. Status of Consultant.....	6
Section 10. Compliance with Applicable Laws and California Labor Code.	7
Section 11. Conflicts of Interest.....	8
Section 12. Confidential Information; Release of Information.	8
Section 13. Indemnification.	9
Section 14. Insurance.	10
Section 15. Assignment.	10
Section 16. Termination of Agreement.....	11
Section 17. Notices.	11
Section 18. General Provisions.....	12
Exhibit "A" Task Order	
Exhibit "B" Key Personnel	
Exhibit "C" Insurance	

AGREEMENT FOR PROFESSIONAL SERVICES

This AGREEMENT FOR PROFESSIONAL SERVICES ("Agreement") effective as of this 1st day of October, 2026 ("Effective Date") is by and between West Valley Water District ("District") and SDI Presence, LLC ("Consultant"). The District and Consultant may be collectively referred to as the "Parties" and individually as a "Party."

RECITALS

A. The Parties desire to enter into this Agreement for the purpose of setting forth the terms and conditions upon which Consultant shall provide certain services to District.

NOW, THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:

Section 1. Term of Agreement.

- (a) Subject to subsection (b) below, the term of this Agreement will be for a period of one (1) year commencing on the Effective Date and terminating one (1) year after the Effective Date.
- (b) This Agreement shall renew automatically for continuous one (1) year periods for no more than two (2) additional years, unless either Party, prior to the end of the existing one (1) year period, delivers written notice to the other Party, that the Agreement shall not be extended.
- (c) If a Task Order (as defined herein) is in effect at the expiration of the term of this Agreement, the term of this Agreement will automatically extend until Consultant completes the services under said Task Order, or until the Agreement is otherwise terminated, as set forth herein.

Section 2. Scope and Performance of Services.

- 2.1** (a) District may, from time to time, by written instructions from the District's General Manager or Assistant General Manager, or their designee, ("Authorized Representative") issue task orders ("Task Orders") to the Consultant. The Task Order shall be in such form and content as shall be set forth on Exhibit "A" attached hereto and by this reference incorporated herein. The Task Order shall set forth: (1) the scope of services to be performed by Consultant; (2) the compensation to be paid to Consultant; and (3) the time to complete the Task Order. The provisions of this Agreement shall apply to all such Task Orders.
- (b) For each Task Order, Consultant shall confer, as requested, with District representatives to review progress of work elements, adherence to work schedule, coordination of work, scheduling of review and resolution of problems which may develop.

2.2 Consultant will furnish all of the labor, technical, administrative, professional and other personnel, all supplies and materials, equipment, printing, vehicles, transportation, office space and facilities, and all tests, testing and analyses, calculation, and all other means whatsoever, except as otherwise expressly specified in this Agreement, necessary or proper to perform and complete the services required of Consultant under this Agreement.

2.3 Consultant's designated representative(s) who are authorized to act on its behalf and to make all decisions in connection with the performance of services under this Agreement are listed in Exhibit "B" attached hereto and by this reference incorporated herein ("Key Personnel"). Consultant shall not substitute or remove Key Personnel without the prior written consent of District.

2.4 Consultant represents and warrants that it has the qualifications, experience, and facilities necessary to properly perform the services required under this Agreement in a thorough, competent, and professional manner. Notwithstanding Section 3 below, in the event Consultant utilizes the services of subcontractors or sub-consultants, Consultant assumes sole and complete responsibility for the performance of the subcontractor or sub-consultant to the specifications provided hereunder for Consultant's work, and no adjustment will be made to Consultant's requirements under this Agreement for timely completion of services, complete performance of services, or delivery of products or deliverables in a timely fashion, and no adjustment will be made to performance deadlines, or compensation due to Consultant, due to or arising from issues Consultant may have with any subcontractor or sub-consultant. Consultant will at all times faithfully, competently and to the best of its ability, experience and talent, perform all services described in this Agreement. In meeting its obligations under this Agreement, Consultant shall employ, at a minimum, generally accepted standards and practices utilized by persons engaged in providing services similar to those required of Consultant under this Agreement.

- (1) Consultant warrants it will perform its services, as more particularly described in this Agreement and each Task Order in accordance with generally accepted professional practices and current standards of care and diligence normally practiced by members of the profession currently practicing under conditions of a similar nature. Consultant shall perform, at its own cost and expense and without reimbursement from the District, any services necessary to correct errors or omissions which are caused by the Consultant's failure to comply with the standard of care provided for herein.

2.5 Neither District nor Consultant shall be considered in default of this Agreement for delays in performance caused by circumstances beyond the reasonable control of the non-performing party. For purposes of this

Agreement, such circumstances include a Force Majeure Event. A Force Majeure Event shall mean an event that materially affects the Consultant's performance and is one or more of the following: (1) Acts of God or other natural disasters occurring at the project site; (2) terrorism or other acts of a public enemy; (3) orders of governmental authorities (including, without limitation, unreasonable and unforeseeable delay in the issuance of permits or approvals by governmental authorities that are required for the services); and (4) pandemics, epidemics or quarantine restrictions. For purposes of this section, "orders of governmental authorities," includes ordinances, emergency proclamations and orders, rules to protect the public health, welfare and safety. Should such a Force Majeure Event occur, the non-performing party shall, within a reasonable time of being prevented from performing, give written notice to the other party describing the circumstances preventing continued performance and the efforts being made to resume performance of this Agreement. Delays shall not entitle Consultant to any additional compensation regardless of the Party responsible for the delay. Notwithstanding the foregoing, District may still terminate this Agreement in accordance with the termination provisions of this Agreement.

Section 3. Additional Services and Changes in Services

3.1 Consultant will not be compensated for any services rendered in connection with its performance of this Agreement that are in addition to or outside of those set forth in the Task Orders unless such additional services are authorized in advance and in writing by District.

3.2 If Consultant believes that additional services are needed to complete a Task Order, Consultant will provide the Authorized Representative with written notification describing the proposed additional services, the reasons for such services, and a detailed proposal regarding cost.

3.3 District may order changes to a Task Order, consisting of additions, deletions, or other revisions, and the compensation to be paid Consultant will be adjusted accordingly. All such changes must be authorized in writing and executed by Consultant and District. The cost or credit to District resulting from changes in a Task Order will be determined by the written agreement between the Parties.

Section 4. Familiarity with Services and Site

4.1 By executing this Agreement, Consultant warrants that Consultant shall, prior to undertaking a Task Order:

- (a) investigate and consider the services to be performed;

- (b) carefully consider how and within what time frame the services should be performed;
- (c) understand the facilities, difficulties, and restrictions attending performance of the services under a Task Order; and
- (d) possesses all licenses required under local, state or federal law to perform the services contemplated by a Task Order and maintain all required licenses during the performance of such Task Order.

4.2 If services involve work upon any site, Consultant warrants that Consultant has or will investigate the site and will be fully acquainted with the conditions there existing, before commencing its services under a Task Order. Should Consultant discover any latent or unknown conditions that may materially affect the performance of services, Consultant will immediately inform District of such fact and will not proceed except at Consultant's own risk until written instructions are received from the District.

Section 5. Compensation and Payment.

5.1 In no event shall the total amount paid for services rendered by Consultant under this Agreement and all Task Orders issued hereunder exceed the sum of the Task Orders. Subject to any limitations set forth in this Agreement, District agrees to pay Consultant the amounts shown in a Task Order.

5.2 Consultant shall furnish District monthly with an original invoice for all services performed and expenses incurred under a Task Order during the preceding month in accordance with the fee schedule set forth in the Task Order. The invoice must detail charges by the following categories: labor (by subcategory), reimbursable costs, subcontractor contracts and miscellaneous expenses. The invoice must list, as applicable, the hours worked and hourly rates for each personnel category, the tasks performed, the percentage of the task completed during the billing period, the cumulative percentage completed for each task, and the total cost of the services.

5.3 District will independently review each invoice submitted by Consultant to determine whether the work performed and expenses incurred are in compliance with this Agreement and the Task Order. In the event that no charges or expenses are disputed, the invoice will be approved and paid. In the event any charges or expenses are disputed by District, the original invoice will be returned by District to Consultant for correction and resubmission.

5.4 Except as to any charges for work performed or expenses incurred by Consultant that are disputed by District, District will use its best

efforts to cause Consultant to be paid within thirty (30) days of receipt of Consultant's invoice.

5.5 No payment or partial payment to Consultant shall constitute acceptance of any work completed by Consultant or waive any claims by the District for any reason whatsoever.

Section 6. Required Documentation Prior to Performance.

6.1 Consultant will not perform any services under this Agreement until:

(a) Consultant furnishes proof of insurance ("Insurance") as required under Exhibit "C" attached hereto and by this reference incorporated herein; and

(b) Consultant provides District with a Taxpayer Identification Number.

6.2 The District will have no obligation to pay for any services rendered by Consultant in advance of receiving written authorization to proceed for each Task Order, and Consultant acknowledges that any such services are at Consultant's own risk.

Section 7. Project Documents.

7.1 All original maps, models, designs, drawings, photographs, studies, surveys, reports, data, notes, computer programs, files and other documents (collectively, "Project Documents") prepared, developed or discovered by Consultant in the course of providing services under this Agreement will become the sole property of District and may be used, reused or otherwise disposed of by District without the permission of Consultant. Consultant will take such steps as are necessary to perfect or protect the ownership interest of District in such Project Documents. Upon completion, expiration or termination of this Agreement, Consultant shall turn over to District all such original Project Documents in its possession; provided, however, that Consultant may retain copies of Project Documents.

7.2 Except as necessary for the performance of services under this Agreement, no Project Documents prepared under this Agreement, will be released by Consultant to any other person or entity without District's prior written approval. All press releases, including graphic display information to be published, must be approved and distributed solely by District, unless otherwise agreed to in writing by District.

Section 8. Consultant's Books and Records.

8.1 Consultant shall maintain any and all documents and records demonstrating or relating to Consultant's performance of services under this

Agreement. Consultant shall maintain any and all ledgers, books of account, invoices, vouchers, canceled checks, or other documents or records evidencing or relating to work, services, expenditures and disbursements charged to District under this Agreement. Any and all such documents or records must be maintained in accordance with generally accepted accounting principles and must be sufficiently complete and detailed so as to permit an accurate evaluation of the services provided by Consultant under this Agreement. Any and all such documents or records must be maintained for three (3) years following the final payment for each Task Order.

8.2 Any and all records or documents required to be maintained by this section must be made available for inspection, audit and copying, at any time during regular business hours, upon written request by District or its designated representatives. Copies of such documents or records must be provided directly to District for inspection, audit and copying when it is practical to do so; otherwise, unless an alternative is mutually agreed upon, such documents and records must be made available at Consultant's address indicated for receipt of notices in this Agreement.

8.3 Where District has reason to believe that any of the documents or records required to be maintained by this section may be lost or discarded due to dissolution or termination of Consultant's business, District may, by written request, require that custody of such documents or records be given to a person or entity mutually agreed upon and that such documents and records thereafter be maintained by such person or entity at Consultant's expense. Access to such documents and records shall be granted to District, as well as to its successors-in-interest and authorized representatives.

Section 9. Status of Consultant.

9.1 Consultant is and will at all times remain a wholly independent contractor and not an officer or employee of District. Consultant has no authority to bind District in any manner, or to incur any obligation, debt or liability of any kind on behalf of or against District, whether by contract or otherwise, unless such authority is expressly conferred under this Agreement or is otherwise expressly conferred in writing by District.

9.2 The personnel performing the services under this Agreement on behalf of Consultant will at all times be under Consultant's exclusive direction and control. Neither District, nor any elected or appointed boards, officers, officials, employees or agents of District, will have control over the conduct of Consultant or any of Consultant's officers, subcontractors or sub-consultants, employees or agents, except as provided in this Agreement. Consultant warrants that it will not at any time or in any manner represent

that Consultant or any of Consultant's officers, employees or agents are in any manner officials, officers, employees or agents of District.

9.3 Neither Consultant, nor any of Consultant's officers, employees or agents, will obtain any rights to retirement, health care or any other benefits which may otherwise accrue to District's employees. Consultant expressly waives any claim to any such rights or benefits.

Section 10. Compliance with Applicable Laws and California Labor Code.

10.1 Consultant shall keep itself informed of and comply with all applicable federal, state and local laws, statutes, codes, ordinances, regulations and rules in effect during the term of this Agreement.

10.2 Consultant is aware of the requirements of California Labor Code Sections 1720 et seq. and 1770 et seq., which require the payment of prevailing wage rates and the performance of other requirements on certain "public works" and "maintenance" projects ("Prevailing Wage Laws"). If the services are being performed as part of an applicable "public works" or "maintenance" project, as defined by the Prevailing Wage Laws, and if the total compensation is \$1,000 or more, Consultant agrees to fully comply with such Prevailing Wage Laws. Consultant shall defend, indemnify and hold the District, its officials, officers, employees and agents free and harmless from any claims, liabilities, costs, penalties or interest arising out of any failure or alleged failure to comply with the Prevailing Wage Laws. It shall be mandatory upon the Consultant and all subconsultants to comply with all California Labor Code provisions, which include but are not limited to prevailing wages (Labor Code Sections 1771, 1774 and 1775), employment of apprentices (Labor Code Section 1777.5), certified payroll records (Labor Code Sections 1771.4 and 1776), hours of labor (Labor Code Sections 1813 and 1815) and debarment of contractors and subcontractors (Labor Code Section 1777.1). The requirement to submit certified payroll records directly to the Labor Commissioner under Labor Code section 1771.4 shall not apply to work performed on a public works project that is exempt pursuant to the small project exemption specified in Labor Code Section 1771.4.

10.3 If the services are being performed as part of an applicable "public works" or "maintenance" project, then pursuant to Labor Code Sections 1725.5 and 1771.1, the Consultant and all subconsultants performing such services must be registered with the Department of Industrial Relations. Consultant shall maintain registration for the duration of the Agreement and require the same of any subconsultants, as applicable. This Agreement may also be subject to compliance monitoring and enforcement by the Department of Industrial Relations. It shall be Consultant's sole responsibility to comply with all applicable registration and labor compliance requirements. Notwithstanding the foregoing, the contractor registration requirements mandated by Labor Code Sections 1725.5 and 1771.1 shall not apply to work performed on a public works project that is exempt pursuant to the small project exemption specified in Labor Code Sections 1725.5 and 1771.1.

10.4 This Agreement may also be subject to compliance monitoring and enforcement by the Department of Industrial Relations. It shall be Consultant's sole responsibility to comply with all applicable registration and labor compliance requirements. Any stop orders issued by the Department of Industrial Relations against Consultant or any subcontractor that affect Consultant's performance of services, including any delay, shall be Consultant's sole responsibility. Any delay arising out of or resulting from such stop orders shall be considered Consultant caused delay and shall not be compensable by the District. Consultant shall defend, indemnify and hold the District, its officials, officers, employees and agents free and harmless from any claim or liability arising out of stop orders issued by the Department of Industrial Relations against Consultant or any subcontractor.

Section 11. Conflicts of Interest.

Consultant covenants that neither Consultant, nor any officer, principal nor employee of its firm, has or will acquire any interest, directly or indirectly, that would conflict in any manner with the interests of District or that would in any way hinder Consultant's performance of services under this Agreement. Consultant further covenants that neither Consultant, nor any officer, principal or employee of its firm will make, participate in the making, or in any way attempt to use the position of Consultant to influence any decision of the District in which Consultant knows or has reason to know that Consultant, or any officer, principal or employee of Consultant has a financial interest as defined in Government Code section 87103.

Section 12. Confidential Information; Release of Information.

12.1 All information gained or work product produced by Consultant in performance of this Agreement will be considered confidential to the full extent permitted by law, unless such information is in the public domain or already known to Consultant. Consultant shall not release or disclose any such information or work product to persons or entities other than District without prior written authorization from an Authorized Representative, except as may be required by law.

12.2 Consultant, its officers, employees, or agents, shall not, without prior written authorization from an Authorized Representative or unless requested by the District counsel, voluntarily provide declarations, letters of support, testimony at depositions, response to interrogatories or other information concerning the work performed under this Agreement. Response to a subpoena or court order will not be considered "voluntary" provided Consultant gives District notice of such court order or subpoena.

12.3 If Consultant, or any officer, employee, or agent of Consultant, provides any information or work product (including Project Documents) in violation of this Agreement, then District shall have the right to reimbursement and indemnity from Consultant for any damages, costs and fees, including attorneys' fees related to any unauthorized disclosure by consultant or, caused by or incurred as a result of Consultant's conduct.

12.4 Consultant shall promptly notify District should, Consultant, its officers, employees, or agents be served with any summons, complaint, subpoena, notice of deposition, request for documents, interrogatories, request for admissions or other discovery request, court order or subpoena from any party regarding this Agreement and the services performed under this Agreement. District retains the right, but has no obligation, to represent Consultant or be present at any deposition, hearing or similar proceeding. Consultant agrees to cooperate fully with District and to provide District with the opportunity to review any response to discovery requests provided by Consultant. However, this right to review any such response does not imply or mean the right by District to control, direct, or rewrite such response.

Section 13. Indemnification.

13.1 Consultant covenants and agrees that, during the term of this Agreement, any injury suffered as a result of Consultant's services shall be the sole responsibility of Consultant and its successors and assigns and District shall not be liable to Consultant, or any other person or persons whatsoever for any such injury, loss or damage to persons or property unless caused by the sole negligence or intentional acts of District or its Representatives (as solely defined below).

13.2 To the fullest extent permitted by law, Consultant shall defend, indemnify and hold District, its officers, directors and Representatives ("District Indemnitees") harmless from and against any and all claims, costs, liabilities, debts, demands, suits, actions, causes of action, obligations, proceedings, damages, judgments, liens and expenses of whatever nature, including attorneys' fees and disbursements (collectively, "Claims") which may be made against the District Indemnitees arising out of or in connection with (a) the retention by District of Consultant's services; (b) the performance of or failure to perform, the services covered by this Agreement which is caused or occasioned by any act, action, neglect on the part of Consultant, or its Representatives, in the performance of this Agreement and the services provided under this Agreement; (c) the death and/or injury to any person or damage to any property (real or personal) and/or economic loss which may be caused or is claimed to have been caused, by the negligence, act or omission of Consultant or its Representatives ; (d) any violation or alleged violation by Consultant of any law or regulation now or hereafter enacted; and (e) any breach by Consultant of its obligations under this Agreement. The foregoing indemnity shall not apply to the extent any such Claims are ultimately established by a court of competent jurisdiction to have been caused by the sole negligence or willful misconduct of the District Indemnitees or any of them. District shall make all decisions with respect to its representation in any legal proceeding concerning this section. If Consultant fails to do so, District shall have the right, but not the obligation, to defend the Claim and charge

all of the direct or incidental costs of such defense, including attorneys' fees and costs, to Consultant and to recover the same from Consultant. The term "Representatives" shall mean employees, representatives, agents, contractors, subcontractors or any other persons directly or indirectly employed by any one of the foregoing or reasonably under the control of any of the foregoing or for whose acts any of the foregoing may be liable.

13.3 If Consultant's obligation to defend, indemnify, and/or hold harmless arises out of Consultant's performance of "design professional" services (as that term is defined under Civil Code section 2782.8), then, and only to the extent required by Civil Code section 2782.8, which is fully incorporated herein, Consultant's indemnification obligation shall be limited to claims that arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of the Consultant, and, upon Consultant obtaining a final adjudication by a court of competent jurisdiction, Consultant's liability for such claim, including the cost to defend, shall not exceed the Consultant's proportionate percentage of fault.

Section 14. Insurance.

Consultant agrees to obtain and maintain in full force and effect during the term of this Agreement the insurance coverages listed in Exhibit "C." All insurance policies shall be subject to approval by District as to form and content. These requirements are subject to amendment or waiver if so approved in writing by an Authorized Representative.

Section 15. Assignment.

15.1 The expertise and experience of Consultant are material considerations for this Agreement. District has an interest in the qualifications of and capability of the persons and entities that will fulfill the duties and obligations imposed upon Consultant under this Agreement. Consultant may not assign or transfer this Agreement or any portion of this Agreement or the performance of any of Consultant's duties or obligations under this Agreement without the prior written consent of District. The District can withhold its approval/consent in its sole and absolute discretion. Any attempted assignment will be null and void, and will constitute a material breach of this Agreement entitling District to any and all remedies at law or in equity, including summary termination of this Agreement.

15.2 Consultant must obtain District's prior written approval before utilizing any subcontractors to perform any services under this Agreement, which said approval may be withheld in District's sole and absolute discretion. This written approval must include the identity of the subcontractor and the terms of compensation. Approval by District does not imply any agreement to or endorsement by the District as to the competency or capability of any proposed subcontractor or sub-consultant, and District

reserves any and all rights against both Consultant and such subcontractor or sub-consultant, for any failure to perform or other breach of any of the provisions of this Agreement, or the standards of performance defined herein, and no waiver is intended or to be implied by District's approval of any subcontractor or sub-consultant.

Section 16. Termination of Agreement.

16.1 District may terminate this Agreement, with or without cause, at any time by giving ten (10) calendar days written notice of termination to Consultant. In the event such notice is given, Consultant shall cease immediately all work in progress.

16.2 Upon termination of this Agreement, all property belonging exclusively to District which is in Consultant's possession, including, but not limited to, Project Documents must be returned to District immediately. Consultant shall promptly deliver to District a final invoice for all outstanding services performed and expenses incurred by Consultant as of the date of termination. If said termination occurs prior to completion of any Task Order for which a payment request has not been received, the charge for services performed during such task shall be the reasonable value of such services, based on an amount mutually agreed to by District and Consultant of the portion of such Task Order completed but not paid prior to said termination.

16.3 Consultant acknowledges District's right to terminate this Agreement as provided in this section, and hereby waives any and all claims for damages that might otherwise arise from District's termination of this Agreement. District shall not be liable for any costs other than the charges or portions thereof which are specified herein. Consultant shall not be entitled to payment for unperformed services, and shall not be entitled to damages or compensation for termination of work.

Section 17. Notices.

17.1 All written notices required or permitted to be given under this Agreement will be deemed made when received by the other Party at its respective address as follows:

To District: West Valley Water District
 855 West Base Line Road
 P. O. Box 920
 Rialto, CA 92377
 Attention: General Manager

 (Tel.) 909-875-1804
 (Fax) 909-875-1849

To Consultant: SDI Presence, LLC
Attention: Shoma Meyer, CFO
Address: 200 E. Randolph Street, Suite 3550
Chicago, IL 60601
Phone Number: 714-975-4150
Email: smeyer@sdipresence.com

**** Please send all invoices by:**

Email: apinvoices@wvwd.org

or

Mail: *West Valley Water District
Accounts Payable
P.O. Box 190
Rialto, CA 92377*

17.2 Notice will be deemed effective on the date personally delivered or transmitted by facsimile. If the notice is mailed, notice will be deemed given three (3) days after deposit of the same in the custody of the United States Postal Service, postage prepaid, for first class delivery, or upon delivery if using a major courier service with tracking capabilities.

17.3 Any Party may change its notice information by giving notice to the other Party in compliance with this section.

Section 18. General Provisions.

18.1 Authority to Execute. Each Party represents and warrants that all necessary action has been taken by such Party to authorize the undersigned to execute this Agreement and to bind it to the performance of its obligations hereunder.

18.2 Binding Effect. Subject to Section 15, this Agreement is binding upon the heirs, executors, administrators, successors and assigns of the Parties, including any subcontractors or sub-consultants of Consultant.

18.3 Entire Agreement. This Agreement and all attachments contain the entire, complete, final and exclusive agreement and understanding of the Parties with respect to the matters addressed in this Agreement and supersedes all other agreements or understandings, whether oral or written, between Consultant and District prior to the execution of this Agreement.

18.4 Modification of Agreement. No amendment to or modification of this Agreement will be valid unless made in writing and approved by Consultant and approved in writing by the Board of Directors of the District,

or in writing by the General Manager, if such power has been delegated to General Manager. The Parties agree that this requirement for written modifications cannot be waived and that any attempted waiver will be void.

18.5 Facsimile Signatures. Amendments to this Agreement will be considered executed when the signature of a Party is delivered by facsimile transmission. Such facsimile signature will have the same effect as an original signature.

18.6 Waiver. Waiver by any Party to this Agreement of any term, condition, or covenant of this Agreement will not constitute a waiver of any other term, condition, or covenant. Waiver by any Party of any breach of the provisions of this Agreement will not constitute a waiver of any other provision, or a waiver of any subsequent breach or violation of any provision of this Agreement. Acceptance by District of any services by Consultant will not constitute a waiver of any of the provisions of this Agreement.

18.7 Interpretation. This Agreement will be interpreted, construed and governed according to the laws of the State of California. Each Party has had the opportunity to review this Agreement with legal counsel. The Agreement will be construed simply, as a whole, and in accordance with its fair meaning, and without resort to rules regarding draftsmanship. It will not be interpreted strictly for or against either Party.

18.8 Severability. If any provision of this Agreement shall be ruled invalid, illegal or unenforceable, the Parties shall: (a) promptly negotiate a substitute for the provisions which shall to the greatest extent legally permissible, effect the intent of the Parties in the invalid, illegal or unenforceable provision, and (b) negotiate such changes in, substitutions for or additions to the remaining provisions of this Agreement as may be necessary in addition to and in conjunction with subsection (a) above to give effect to the intent of the Parties without the invalid, illegal or unenforceable provision. To the extent the Parties are unable to negotiate such changes, substitutions or additions as set forth in the preceding sentence, and the intent of the Parties with respect to the essential terms of the Agreement may be carried out without the invalid, illegal or unenforceable provisions, the balance of this Agreement shall not be affected, and this Agreement shall be construed and enforced as if the invalid, illegal or unenforceable provisions did not exist.

18.9 Venue. The Parties agree any action or proceeding to enforce or relating to this Agreement shall be brought exclusively in the federal court located in Riverside County, California or state court located in San Bernardino County, California and the Parties hereto consent to the exercise of personal jurisdiction over them by such courts for purposes of any such action or proceeding.

18.10 Disputes. If any disputes should arise between the Parties concerning the work to be done under this Agreement, the payments to be made, or the manner of accomplishment of the work, Consultant shall nevertheless proceed to perform the work as directed by District pending settlement of the dispute.

18.11 Cooperation. Consultant shall cooperate in the performance of work with District and all other agents.

18.12 Time of Essence. Time shall be of the essence as to all dates and times of performance contained in this Agreement.

18.13 Counterparts. This Agreement may be signed and delivered in any number of counter parts, each of which, when signed and delivered, shall be an original, but all of which shall together constitute one and the same Agreement.

[SIGNATURES APPEAR ON FOLLOWING PAGE]

**SIGNATURE PAGE FOR AGREEMENT FOR PROFESSIONAL SERVICES
BETWEEN THE WEST VALLEY WATER DISTRICT
AND SDI PRESENCE, LLC**

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed effective as of the day and year first above written.

Each Party acknowledges and agrees that this Agreement may be executed by electronic or digital signature, which shall be considered as an original signature for all purposes and shall have the same force and effect as an original signature.

DISTRICT:

**WEST VALLEY WATER DISTRICT,
a public agency of the State of California**

By _____
John Thiel, General Manager

CONSULTANT:

SDI Presence, LLC

By	_____
Name	Shoma Meyer
Its	Chief Financial Officer

EXHIBIT A
TASK ORDER

TASK ORDER NO. 1

This Task Order ("Task Order") is executed this 1st day of October, 2026 by and between West Valley Water District, a public agency of the State of California ("District") and **SDI Presence, LLC** ("Consultant").

RECITALS

- A. On or about October 1, 2026 District and Consultant executed that certain Agreement for Professional Services ("Agreement").
- B. The Agreement provides that the District will issue Task Orders from time to time, for the provision of certain services by Consultant.
- C. Pursuant to the Agreement, District and Consultant desire to enter into this Task Order for the purpose of setting forth the terms and conditions upon which Consultant shall render certain services to the District.

NOW, THEREFORE, THE PARTIES HERETO HEREBY AGREE AS FOLLOWS:

- 1. Consultant agrees to perform the services set forth on Exhibit "1" attached hereto and by this reference incorporated herein.
- 2. Subject to any limitations in the Agreement, District shall pay to Consultant the amounts specified in Exhibit "2" attached hereto and by this reference incorporated herein. The total compensation, including reimbursement for actual expenses, may not exceed the amount set forth in Exhibit "2," unless additional compensation is approved in writing by the District.
- 3. Consultant shall perform the services described in Exhibit "1" in accordance with the schedule set forth in Exhibit "3" attached hereto and by this reference incorporated herein. Consultant shall commence work immediately upon receipt of a notice to proceed from the District. District will have no obligation to pay for any services rendered by Consultant in advance of receipt of the notice to proceed, and Consultant acknowledges that any such services are at Consultant's own risk.
- 4. The provisions of the Agreement shall apply to this Task Order. As such, the terms and conditions of the Agreement are hereby incorporated herein by this reference.

[SIGNATURES APPEAR ON FOLLOWING PAGE]

IN WITNESS WHEREOF, the parties have caused this Task Order to be executed effective as of the day and year first above written.

DISTRICT:

**WEST VALLEY WATER DISTRICT,
a public agency of the State of California**

John Thiel, General Manager

CONSULTANT:

SDI Presence, LLC

By	_____
Name	Shoma Meyer
Its	Chief Financial Officer

EXHIBIT “1”

TO

TASK ORDER NO. 1

SCOPE OF SERVICES

- Comprehensive assessment of IT infrastructure, including networks, servers, hardware life cycles, storage, cloud services, and cybersecurity posture.
- Review of core business applications (ERP, financial systems, customer billing, GIS, SCADA/OT).
 - Note: a SCADA Master Plan is in the final draft stages and will be available for reference.
- Review of current licensing.
- Analysis of data management practices, integration, and business intelligence capabilities.
- Evaluation of staffing levels, skillsets, training, and IT governance structure.
- Development of a prioritized list of IT projects with estimated budgets and implementation timelines.
- Recommendations for additional business applications.
- Recommendations for disaster recovery, business continuity, and incident response planning.
- Identification of opportunities to leverage emerging technologies (cloud, mobile, AI, IoT) for improved delivery service.
- A comprehensive IT Master Plan with a five-year horizon, including narrative analysis and supporting exhibits.
- A project portfolio with prioritized initiatives, cost estimates, and timelines.
- Documentation of stakeholder engagement and needs assessment results, (to include network diagrams, application lists, etc.).
- Recommendations for IT specific policies.
- Recommendations for organizational structure, staffing, and training enhancements for both IT staff and staff in general.
- A final presentation to executive staff and the Board summarizing key outcomes and action items.



Proposal Prepared For:

West Valley Water District

IT Master Plan

RFP #2026-06



Respectfully Submitted By:



Patrick Griffin

Managing Director

pgriffin@sdipresence.com

714-975-4150

Cover Letter

July 30, 2026

Ms. Luz Granados, Support Services Supervisor
West Valley Water District
855 West Base Line Road
Rialto, CA 92377

Re: RFP No. 2026-06 – IT Master Plan

Dear Ms. Granados:

SDI Presence LLC (SDI) respectfully submits this proposal to the West Valley Water District (WVWD) in response to Request for Proposal No. 2026-06 for Professional Services to Develop an Information Technology (IT) Master Plan. SDI is a limited liability company headquartered at 200 E. Randolph Street, Suite 3550, Chicago, Illinois 60601, with regional offices in Los Angeles and Sacramento. WVWD's project will be led from our Anaheim office located at 4368 E. La Palma Avenue, Anaheim, California 92807.

Since 1996, SDI has provided management consulting services focused exclusively on helping public sector organizations strategically leverage and manage technology. Our team has supported more than 200 government and utility clients nationwide through IT assessments, strategic and master planning initiatives, technology procurements, cybersecurity evaluations, organizational assessments, and implementation support. We have successfully completed more than 100 IT Assessments and Strategic Plans for local government agencies, providing us with the expertise necessary to help WVWD evaluate its current IT environment and develop a practical, actionable five-year IT Master Plan aligned with the District's Strategic Plan and business objectives.

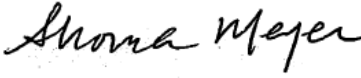
SDI understands the importance of a comprehensive assessment of WVWD's technology landscape, including infrastructure, cloud services, cybersecurity, business applications, data management practices, IT governance, staffing, and operational technologies. Our proven methodology will provide an independent evaluation of the District's current-state environment, including core systems such as ERP, financial systems, customer billing, GIS, and SCADA/OT platforms. We will identify opportunities to strengthen cybersecurity, enhance operational efficiency, improve business continuity and disaster recovery capabilities, and leverage emerging technologies such as cloud, mobile, artificial intelligence, and IoT solutions to support future service delivery.

SDI brings WVWD a structured, public-sector-focused approach grounded in industry best practices, including Information Technology Infrastructure Library (ITIL)-based IT Service Management (ITSM), cybersecurity frameworks, and technology governance standards. Our deliverables will include a prioritized portfolio of initiatives, budgetary planning considerations, implementation timelines, organizational and staffing recommendations, and a comprehensive roadmap designed to support the District's technology investments over the next five years.

Our Advisory & Consulting practice is proud to be 100% vendor independent. We maintain no partnerships, reseller relationships, or financial affiliations with hardware or software vendors. This independence ensures that all recommendations are objective, strategic, and based solely on the best interests of WVWD.

SDI appreciates the opportunity to submit our proposal to West Valley Water District for this important initiative. We look forward to partnering with the District to develop a forward-looking IT Master Plan that supports reliable, secure, and resilient technology services for years to come. If you have any questions regarding our proposal, please contact SDI Managing Director Patrick Griffin at (714) 975-4150 or pgriffin@sdipresence.com. Mr. Griffin is responsible for the contents of this proposal and is authorized to negotiate a contract on behalf of SDI. As Chief Financial Officer of SDI, I am authorized to bind the company.

Sincerely,

A handwritten signature in black ink that reads "Shoma Meyer".

Shoma Meyer

Chief Financial Officer
SDI Presence LLC

Table of Contents

Cover Letter.....	i
Section I Statement of Qualifications.....	1
Section II Methodology and Approach.....	6
Section III Pricing.....	19
Appendix A – Advisory & Consulting Client List.....	20
Appendix B – Project Team Resumes.....	25
Appendix C Legal Exceptions.....	38

Section I Statement of Qualifications

SDI Presence LLC (SDI)

SDI is an IT consultancy and managed services provider (MSP) that leverages its strong team presence to advance our clients to a secure digital enterprise. With a **30+ year corporate resume**, SDI delivers strategic managed services, IT consulting, and hybrid infrastructure solutions to optimize our clients' technological environments. SDI is a certified Minority Business Enterprise (MBE), with a portfolio of clients that includes some of the nation's largest airports, utilities, commercial real estate portfolios, and government agencies.

SDI delivers a deep technical presence through a local delivery model to achieve customer confidence and success. SDI is headquartered in Chicago, Illinois with regional offices in Anaheim and Sacramento, California; Atlanta, Georgia; and Dallas/Fort-Worth, Texas.

SDI Snapshot:

- Headquartered in Chicago
- 30+ Years IT Consulting/Systems Integration/Implementation Experience
- 400+ Business Professionals
- 87% Customer Satisfaction Rating / 89 Promoter Score
- Continuously awarded the "Best Places to Work" Recognition since 2018
- Financial Stability:
 - 2025 Revenue - \$99.18M
 - Backed by Private Equity Firm - Abry Partners with \$5B under management

The services proposed will be provided through SDI's Advisory & Consulting Practice, which specializes in independent, vendor-neutral consulting and project advisory services for public sector organizations. The Advisory & Consulting team regularly provides IT strategic planning, enterprise system procurements, and project management services to local government agencies, and has completed over 100 IT Master Plans.

SDI Core Services



Advisory & Consulting

Expert guidance to help organizations navigate complexity, drive strategy, and achieve operational excellence.



IT Managed Services

Comprehensive IT support ensures reliable operations, enhanced security, and scalable performance through expert management.



Enterprise Data & AI

Transforming enterprise data into actionable insights with AI-driven solutions that accelerate innovation and decision-making.



Public Safety

Mission-critical technology solutions that empower public safety agencies to respond faster, collaborate better, and protect communities.



ServiceNow

Streamlining workflows and boosting productivity with tailored ServiceNow solutions that unify systems and drive digital transformation.



Enterprise Asset Management

Optimizing asset performance and lifecycle management to reduce downtime, control costs, and drive operational efficiency.



SDI offers a broad technical skill set to our clients, offering deep expertise in each stage of the traditional or cloud-based systems lifecycle. SDI brings a well-rounded team of professional business consultants, certified technicians and years of mission-critical IT experience to each of our client engagements.

Unmatched Technical & Industry Expertise

SDI teams bring executive presence and diverse perspective to our clients' most complex projects. Our team of professionals bring previous experience gained from running large IT operations and multimillion-dollar IT projects.

Together, the SDI team has an extensive history of running complex, 24x7 mission-critical IT environments that demand both a broad and deep IT expertise and unwavering commitment to performance excellence – from a comprehensive IT Assessment for a local municipality, to enterprise cybersecurity remediation at a utility, to a 24x7x365 IT managed services program across a large city transit authority. We bring industry subject matter expertise, technical certifications and methodologies, and a desire to make a positive impact at our clients.

What Sets SDI Apart from Other Advisory Firms

SDI's **Advisory & Consulting Practice** has been partnering with local government clients for 30 years, providing technology advisory services to assist organizations increase efficiency by maximizing the use of technology to support best business practices. Our advisory team has worked with more than 200 local government clients to complete technology plans, implement new technology, and maximize the use of existing technology systems.

While our list of satisfied clients is a testament to our success, one of the most compelling aspects that sets SDI's advisory team apart from other consulting firms is the history and background of the team members. Our advisory consultants are seasoned local government professionals: former CIOs, IT Directors, Finance Directors, and City Executives who have experienced the challenges local governments face and who apply their real-world experience to meet the needs of today's clients. This experience is an essential component of the SDI advisory team's success with local government customers.

SDI has the relevant experience and expertise to provide all of the services being requested by the District, and we are prepared to begin the project immediately. It is important to note that SDI's Advisory & Consulting Practice has, and will continue to be, **100% independent from any technology solution provider**. We pride ourselves on this independence and recognize that it is a critical attribute during the IT master planning process.

SDI is recognized throughout the State of California for our services supporting public sector agencies with IT master planning activities. This is evident not only by the number of successful projects and client references, but also because we are commonly asked by organizations such as California Society of Municipal Financial Officers (CSMFO) and Municipal Information Systems Association of California (MISAC) to present at their annual conferences and regional chapter groups. Recently, SDI was invited to co-present two MISAC webinars on the topic of data management and artificial intelligence. The fact that we are continually invited to present at these important organization's events speaks to our expertise and experience.

Qualifications and References

IT Master Planning and Related Technology Experience

SDI's Advisory & Consulting Practice has worked with more than 200 state and local government agencies across eight states to complete IT Assessments, IT Strategic Plans, GIS Strategic Plans, Network Assessments, IT Service-Level Assessments, Policy/Procedure Documentation, Project Management Organization implementations, Feasibility Studies, and Request for Proposal (RFP) Development and Procurement Management efforts. Since 1999, SDI has completed over 100 IT Strategic Plans. In addition to our California local government experience, SDI also has significant planning, project management, and procurement experience working with the State of California for agencies such as California Highway Patrol, Department of Justice, Department of Motor Vehicles, Department of Corrections and Rehabilitation, Department of Child Support Services, and more.

Provided in Appendix A is a comprehensive listing of our Advisory & Consulting clients, along with the type of projects completed for each client. This document provides the District with a complete list of IT Master / Strategic Plans completed.

Table 1 below provides a complete presentation of IT Strategic / Master Plans completed in the past five years. Projects highlighted in blue are still underway.

City of Alameda	City of Arcadia	City of Arroyo Grande
City of Beverly Hills	Central Contra Costa San Dist	Elsinore Valley Water District
City of Gilroy	Helix Water District	City of Hercules
City of Malibu	City of Manteca	City of Palm Springs
City of Placentia	Port of Los Angeles	City of Rocklin
City of Sacramento Utilities	San Diego Comm College Dist	City of San Ramon
Stockton Port District	City of Upland	City of Vista

Table 1 – Strategic / Master Plans in Past Five Years

Provided on the following pages are project profiles for IT Master Plan engagements that are similar in scope and size to the District. Also included is a plan completed for the Central Contra Costa Sanitary District, which was much larger in scope as it included all aspects of IT and OT.

Name of Organization	Rancho California Water District	
Address	42135 Winchester Road Temecula, CA 92590	
Name of Contact	Patrick Elsasser, Datacenter Operations Supervisor	
Telephone and Email	(951) 296-6998 elsasserp@ranchowater.com	
SDI Resources Assigned	Patrick Griffin – Delivery Executive Lee Curtis – Project Advisor Brian Ganley – Project Consultant	
Completion Date & Cost	June 2025 \$59,040	
IT Assessment & IT Master Plan SDI completed a comprehensive assessment of the District’s technology operations and provided recommendations designed to improve overall service delivery. SDI also developed a Technology Master Plan to guide the District’s future technology investments.		

Name of Organization	Elsinore Valley Water District	
Address	31315 Chaney Street Lake Elsinore, CA 92530	
Name of Contact	Darryn Flexman, Director of Information Technology	
Telephone and Email	(951) 674-3146 Ext. 8255 dflexman@evmwd.net	
SDI Resources Assigned	Patrick Griffin – Delivery Executive Brian Ganley – Project Consultant	
Completion Date & Cost	November 2022 \$79,175	
IT Assessment & IT Master Plan SDI completed an assessment of the District’s technology operations and developed an IT Master Plan to guide future technology investments. After completing the Plan, SDI was engaged to complete a Disaster Recovery / Business Continuity Plan for the District.		

Section III Pricing

SDI recognizes that the District has indicated that the cost proposal may be submitted with the technical proposal package and is not required as a separate document. However, the PlanetBids submission portal identifies the Cost File as a required upload. Accordingly, SDI will provide its pricing information in a manner that complies with the PlanetBids requirements.

Appendix A - Advisory & Consulting Client List

The following pages provide a representative list of SDI's Advisory & Consulting List for the West Coast, illustrating our broad experience developing IT strategies, roadmaps, and technology transformation programs for organizations with operational and infrastructure requirements similar to those of WVWD.

	IT Strategic Plans	IT Assessments	IT Policies & Procedures	Project Management	IT Governance	Disaster Recovery Planning	System Selection & Procurements	Other Management Consulting
Municipalities								
Alameda, CA	✓	✓					✓	✓
Alhambra, CA			✓					✓
Anaheim, CA	✓			✓			✓	✓
Arcadia, CA	✓		✓					✓
Arroyo Grande, CA	✓	✓						
Belmont, CA	✓							
Benicia, CA				✓				✓
Beverly Hills, CA	✓	✓						✓
Branson, MO	✓	✓						✓
Brentwood, CA	✓	✓						
Burbank, CA	✓	✓					✓	
Burlingame, CA				✓			✓	
Carson, CA				✓				
Carson City, NV	✓	✓					✓	✓
Chino, CA				✓			✓	✓
Chino Hills, CA				✓			✓	✓
Chula Vista, CA								✓
Clovis, CA	✓	✓			✓			
Concord, CA				✓				✓
Coronado, CA			✓	✓			✓	✓
Costa Mesa, CA								✓
Cupertino, CA	✓	✓						
Daly City, CA							✓	
Davis, CA							✓	✓
Downey, CA				✓			✓	
Eastvale, CA							✓	
El Segundo, CA	✓	✓						✓
Fairfield, CA	✓	✓	✓		✓	✓	✓	✓
Fontana, CA		✓						
Folsom, CA	✓	✓			✓			
Fremont, CA				✓			✓	✓
Fresno, CA	✓	✓					✓	✓
Galt, CA	✓	✓	✓	✓	✓	✓	✓	✓

	IT Strategic Plans	IT Assessments	IT Policies & Procedures	Project Management	IT Governance	Disaster Recovery Planning	System Selection & Procurements	Other Management Consulting
Gilroy, CA	✓	✓		✓			✓	✓
Glendale, CA	✓	✓		✓			✓	✓
Glendora, CA			✓					✓
Half Moon Bay, CA				✓			✓	
Hanford, CA				✓				✓
Hawaiian Gardens, CA				✓			✓	
Hayward, CA				✓				✓
Hercules, CA	✓	✓						
Huntington Beach, CA	✓	✓			✓			✓
Indio, CA				✓			✓	✓
Industry, CA				✓				
Irvine, CA		✓		✓	✓	✓		✓
La Quinta, CA				✓			✓	✓
Laguna Beach, CA	✓	✓						
La Verne, CA			✓					✓
Lincoln, CA				✓				
Long Beach, CA				✓			✓	✓
Los Altos, CA				✓				
Los Angeles, CA				✓				✓
Los Banos, CA	✓	✓						
Malibu, CA	✓	✓		✓	✓		✓	✓
Manhattan Beach, CA	✓	✓			✓		✓	✓
Manteca, CA	✓	✓		✓	✓			✓
Merced, CA			✓				✓	✓
Millbrae, CA							✓	
Monterey, CA				✓			✓	
Moreno Valley, CA			✓					✓
Napa, CA	✓	✓			✓			✓
Newport Beach, CA					✓		✓	✓
Norco, CA							✓	✓
Novato, CA	✓	✓			✓			✓
Ontario, CA		✓		✓			✓	
Orange, CA	✓	✓			✓		✓	✓
Oxnard, CA	✓	✓						
Palmdale, CA	✓	✓						
Palm Springs, CA	✓	✓						✓
Pasadena, CA							✓	✓
Paso Robles, CA				✓			✓	✓
Petaluma, CA							✓	
Pico Rivera, CA							✓	
Pismo Beach, CA	✓	✓					✓	

	IT Strategic Plans	IT Assessments	IT Policies & Procedures	Project Management	IT Governance	Disaster Recovery Planning	System Selection & Procurements	Other Management Consulting
Placentia, CA	✓	✓						✓
Pleasant Hill, CA							✓	
Pomona, CA	✓	✓			✓			
Port Angeles, WA	✓	✓						
Poway, CA							✓	
Rancho Cordova, CA	✓	✓						✓
Rancho Cucamonga, CA							✓	✓
Rancho Palos Verdes, CA	✓	✓					✓	✓
Redlands, CA							✓	✓
Redondo Beach, CA		✓						
Redwood City, CA	✓	✓		✓			✓	
Rialto, CA				✓				✓
Ridgecrest, CA	✓	✓			✓			
Riverside, CA							✓	
Rocklin, CA	✓	✓						✓
Rohnert Park, CA	✓			✓			✓	✓
Sacramento, CA	✓	✓			✓			✓
San Bernardino, CA		✓						✓
San Clemente, CA	✓	✓						
San Luis Obispo, CA	✓	✓					✓	✓
San Rafael, CA	✓	✓		✓	✓		✓	✓
San Ramon, CA	✓	✓		✓			✓	
Santa Ana, CA				✓			✓	
Santa Barbara, CA				✓				
Santa Clara, CA	✓	✓	✓	✓	✓		✓	✓
Santa Cruz, CA	✓	✓	✓		✓			✓
Santa Monica, CA								✓
Santa Rosa, CA								✓
Santee, CA				✓			✓	
Scottsdale, AZ				✓			✓	
Seal Beach, CA				✓				
Sonoma, CA				✓				
Stockton, CA	✓	✓		✓	✓			✓
Suisun City, CA				✓			✓	
Sunnyvale, CA							✓	✓
Temecula, CA	✓	✓						
Torrance, CA							✓	
Truckee, CA	✓	✓						
Tustin, CA				✓			✓	
Upland, CA	✓	✓		✓				
Vacaville, CA							✓	

	IT Strategic Plans	IT Assessments	IT Policies & Procedures	Project Management	IT Governance	Disaster Recovery Planning	System Selection & Procurements	Other Management Consulting
Ventura, CA	✓	✓			✓			✓
Vernon, CA				✓				
Visalia, CA	✓	✓			✓			
Vista, CA	✓	✓	✓		✓			✓
Walnut Creek, CA	✓	✓			✓			✓
Watsonville, CA	✓	✓		✓				✓
West Covina, CA			✓				✓	✓
West Hollywood, CA	✓	✓			✓		✓	
Westminster, CA								✓
Yorba Linda, CA				✓				
Yuba City, CA				✓			✓	
Yucaipa, CA				✓				
Special Districts								
Camrosa Water District							✓	
Central Contra Costa Sanitary District	✓	✓	✓	✓	✓			✓
Central Utah Water Conservation District				✓			✓	
Chino Valley Independent Fire District				✓			✓	✓
Citrus Heights Water District								✓
Coachella Valley Water District				✓			✓	✓
Cosumnes Community Services District				✓			✓	
Cucamonga Valley Water District				✓			✓	
Delta Diablo Sanitation District	✓	✓						✓
East Bay Regional Park District				✓			✓	
East Valley Water District	✓	✓						
Eastern Municipal Water District							✓	
Elsinore Valley Municipal Water District	✓	✓				✓		
Encina Wastewater Authority					✓			
Fresno Irrigation District	✓	✓						
Helix Water District	✓	✓			✓	✓		✓
Inland Empire Utilities Agency	✓	✓		✓			✓	✓
Lake Arrowhead Community Services							✓	
Las Virgenes Municipal Water District	✓	✓				✓	✓	
Monterey Regional Water P.C.A.	✓	✓						
Moraga – Orinda Fire District								✓
Moulton Niguel Water District	✓	✓	✓	✓	✓		✓	✓
North Tahoe Public Utilities District	✓	✓						
Port of Los Angeles	✓	✓						
Rancho California Water District	✓	✓			✓			✓
Riverside County Transp. Commission				✓				
Sacramento Area Sewer District								✓
Sacramento Metropolitan Fire District		✓					✓	

	IT Strategic Plans	IT Assessments	IT Policies & Procedures	Project Management	IT Governance	Disaster Recovery Planning	System Selection & Procurements	Other Management Consulting
Sacramento Municipal Utility District								✓
San Bernardino County Fire								✓
San Diego Community College District	✓	✓						
San Joaquin Council of Governments							✓	
San Jose Water								✓
Santa Clara County Fire Department		✓						✓
Santa Clara County Housing Authority	✓	✓						
Santa Clara Valley Water District							✓	
Silicon Valley Clean Water							✓	
Silicon Valley Power	✓			✓			✓	✓
Solano County Transit (SolTrans)								✓
South Tahoe Public Utility District	✓	✓			✓	✓	✓	
Southern CA Association of Governments								✓
Stockton Port District	✓	✓						
West Basin Municipal Water District	✓	✓			✓			
Zone 7 Water Agency	✓	✓						
Counties								
Douglas County, Nevada		✓						✓
El Paso County, Texas	✓	✓						
Lane County, Oregon	✓	✓						
Los Angeles County Employees Retirement							✓	
Los Angeles County Office of Education				✓				
Orange County, CA – John Wayne Airport		✓						
Placer County, CA							✓	✓
Riverside County, CA				✓				✓
San Benito County, CA				✓				✓
San Diego County, CA				✓				✓
Santa Clara County, CA				✓				✓
Sonoma County, CA				✓				✓
Tulare County, CA	✓	✓			✓			✓
State of California								
CA Correctional Health Care Services				✓				✓
CA Dept. of Child Support Services				✓				✓
CA Dept. of Corrections				✓				✓
CA Dept. of Fish and Game				✓				✓
CA Dept. of Health Care Services				✓				✓
CA Dept. of Justice				✓				✓
CA Dept. of Motor Vehicles				✓				✓
CA Dept. of Public Health				✓				✓
CALPERS				✓			✓	✓
California Highway Patrol	✓	✓	✓	✓	✓	✓	✓	✓

Appendix B – Project Team Resumes

The following pages provide resumes for the project team being proposed for the District's engagement.



Patrick Griffin
Managing Director



Experience Summary

Senior public sector and consulting executive with over 31 years of experience in local agency management, advisory services, and operational leadership. Brings deep expertise across municipal finance, information technology, community development, strategic planning, business process analysis, and enterprise system procurement and implementation. Proven in leading assessments, defining requirements, facilitating stakeholder engagement, supporting elected officials, and overseeing complex initiatives that improve service delivery and align technology and operations with organizational priorities in public sector environments.

Professional Experience

SDI

(01/2012 - Present)

Managing Director

- Oversees the Advisory & Consulting practice, providing leadership for public sector technology advisory and consulting engagements.
- Leads and participates in technology service delivery assessments and strategic planning initiatives for numerous public agencies, including cities, water districts, and utility agencies.
- Conducts reviews of technology operations, identifies customer needs, prioritizes initiatives, and develops strategic implementation plans.
- Directs major enterprise system procurements for Enterprise Resource Planning (ERP) and Land Management System (LMS) initiatives for public sector clients.
- Has served as project manager for ERP and Land Management System implementation projects, including engagements for the cities of Manhattan Beach, La Quinta, and Chino.

Local Government

(01/1981 - 12/2011)

Finance Director / City Treasurer / Assistant City Manager

- Built more than 31 years of public sector local agency management experience with responsibility across all aspects of municipal operations.
- Managed annual budgets, public information dissemination, elected official support, and information technology functions.
- Held leadership responsibility for the day-to-day operations of Finance, Information Technology, and Community Development departments within a full-service city.
- Oversaw staff management, strategic planning activities, annual operating and capital budget development, and departmental operations.
- Brought broad knowledge of local government operations, with experience spanning finance, administration, and organizational leadership.

AREAS OF EXPERTISE

- Project Management
- Requirements Definition
- Business Process Analysis
- Project Plan Development
- Local Government Operations
- Strategic Planning
- Initiative Development
- Operational Assessments
- Workshop Facilitation
- IT Outsourcing Evaluations
- Feasibility Studies
- RFP Development
- Proposal Writing
- Contract Negotiations
- Enterprise System Procurements
- ERP Implementations
- Land Management System Implementations
- Public Sector Operations Management
- Budget Development
- Information Technology Oversight



Education

California State Long Beach

Master of Arts, Public Administration

California State Fullerton

Bachelor of Arts, Psychology



Skills

- **Project Management**
 - Project management
 - Project plan development
- **Business Analysis & Planning**
 - Requirements definition
 - Business process analysis
 - Strategic planning
 - Initiative development
 - Operational assessments
 - Feasibility studies
 - Workshop facilitation
- **Public Sector & Municipal Operations**
 - Local government operations
 - Municipal management
 - Annual budget development
 - Capital budget oversight
 - Elected official support
 - Public information dissemination
- **Procurement & Sourcing**
 - IT outsourcing evaluations
 - RFP development
 - Proposal writing
 - Contract negotiations
 - Enterprise system procurements
- **Enterprise Systems**
 - Enterprise Resource Planning (ERP)
 - Land Management Systems (LMS)
- **Functional Areas**
 - Finance
 - Information Technology
 - Community Development



Lee Curtis

Strategic Planning Practice Leader



Experience Summary

Senior technology and management consulting executive with more than 40 years of experience leading technology service delivery, strategic planning, and IT organizational improvement for public sector and other client environments. Brings deep expertise in IT assessments, strategic and operational planning, project and portfolio prioritization, interim IT leadership, and technology roadmap development, with a hands-on approach spanning executive consulting, departmental oversight, infrastructure and application planning, and implementation of IT best practices. Recognized for providing clear recommendations, actionable strategic plans, and effective leadership that strengthen governance, improve service delivery, align technology investments with business priorities, and support organizational transition and long-term operational performance.



Professional Experience

IT Assessment

Mr. Curtis has developed IT Assessments for clients that provide a comprehensive review of management and operation performance of the IT organization. These assessments evaluate the current use of IT best practices in six operational dimensions (IT Governance, Business Application Portfolio, Service Delivery, Security/Data Protection, Infrastructure, and Administration). The assessments also provide actionable recommendations for the improvement and effective operation of the IT organization to more effectively deliver services to consumers given available resources and priorities.

- City of Clovis, CA
- City of Concord, CA
- City of Daly City, CA
- City of Fairfield, CA
- City of Galt, CA
- City of Rocklin, CA
- City of San Clemente, CA
- Douglas County, NV
- John Wayne Airport, CA
- Lane County, OR
- North Tahoe Public Utility District, CA
- Sacramento Area Sewer District, CA
- Sacramento Metropolitan Fire, CA



AREAS OF EXPERTISE

- IT Strategic Planning
- IT Assessments
- Technology Service Delivery Assessments
- IT Governance
- IT Roadmap Development
- Business Process Analysis
- Requirements Definition
- Project Management
- Project Prioritization
- IT Portfolio Management
- Technology Planning and Assessments
- Operational Assessments
- IT Organization Analysis
- IT Best Practices Implementation
- Disaster Recovery Planning
- IT Policy and Procedure Development
- Service Level Measurement
- Data Center Management
- RFP Development
- Contract Negotiation

SKILLS

- IT Strategy & Planning
- IT Management & Governance
- Project & Operational Management
- Consulting & Administrative



IT Assessment and Strategic Plan

Mr. Curtis has led or participated in technology service delivery assessments and strategic planning projects for the following public agencies. All of the projects involved performing a detailed assessment of the use and management of technology operations, identification of departmental technology needs, prioritization of identified projects, and the creation of a strategic implementation plan including timeframes and estimated costs.

- City of Alameda, CA
- City of Branson, MO
- City of Brentwood, CA
- City of Carson City, NV
- Central Contra Costa Water District, CA
- City of Cupertino, CA
- Cosumnes Community Services District, CA
- City of Gilroy, CA
- City of Los Banos, CA
- City of Manhattan Beach, CA
- City of Napa, CA
- City of Novato, CA
- City of Petaluma, CA
- City of Rancho Palos Verdes, CA
- City of Redwood City, CA
- City of San Luis Obispo, CA
- City of Santa Clara, CA
- City of Santa Cruz, CA
- City of Stockton, CA
- City of Visalia, CA
- City of Walnut Creek, CA
- Delta Diablo Sanitation District, CA
- El Paso County, TX
- Fresno Irrigation District
- Monterey One Water, CA
- Moulton Niguel Water District, CA
- Port of Los Angeles, CA
- Santa Clara County Housing Authority
- South Orange County Wastewater, C
- South Tahoe Public Utility District, CA
- Union Sanitary District, CA
- Zone 7 Water Control Agency, CA

IT Roadmap

Mr. Curtis developed application software strategies that mapped the acquisition/upgrade of core business software. These roadmaps were developed in concert with client user departments and included a comprehensive infrastructure analysis of hardware and support equipment requirements. The roadmaps were used to allocate client technology budgets to mission critical projects and provided a platform by which the IT organizations could effectively manage and utilize its resources to meet client business needs.

- California Highway Patrol, CA
- City of Belmont, CA
- City of Los Altos, CA
- City of Rancho Cordova, CA
- City of Temecula, CA
- Metropolitan Transportation Commission, CA
- Sacramento Area Sewer Districts, CA



Education

University of South Dakota

Economics/Business Administration

- **Consulting & Administrative**
 - RFP development
 - Proposal writing
 - Contract negotiation
 - Personnel management
 - P&L administration



Michael Stein
Project Consultant



Experience Summary

Highly experienced management and technology consultant with more than 40 years of success advising public sector, telecommunications, and commercial banking organizations on the effective use of technology to address business needs. Brings deep expertise in IT strategic planning, project management, business process re-engineering, requirements definition, procurement support, governance, and operational assessments, with particular strength in guiding complex technology initiatives, Commercial-Off-The-Shelf system implementations, and information exchange improvements. Recognized for working effectively with executive leadership and key stakeholders to assess current-state capabilities, identify gaps, develop actionable strategies, and improve organizational processes and technology decision-making.

Professional Experience

City of Watsonville: Information Technology Strategic Plan

Project Manager and Lead Consultant

- Led development of the City's IT Strategic Plan and IT classification and compensation study.
- Conducted a detailed assessment of the Information Technology Division, including current challenges, active projects, and improvement opportunities.
- Interviewed key user stakeholders and facilitated planning, prioritization, and IT governance workshops to support strategic decision-making.

Lane County, Oregon: Business Information Technology Assessment

Lead Consultant

- Led an assessment of the County's use of information technology, including IT governance, service management, and service delivery processes.
- Reviewed the methodology and administration of the County's IT chargeback program, including direct and indirect cost allocation to user departments.
- Worked closely with the County Administrator, Chief Information Officer, and key user stakeholders to evaluate conformance to IT best practices, develop a gap analysis, and produce an action plan for County management.

Education

John Jay College of Criminal Justice, CUNY / 1974

Master of Public Administration Program

Marietta College, Ohio / 1972

Bachelor of Arts

AREAS OF EXPERTISE

- Project Management
- IT Governance
- Needs and Gap Analysis
- Business Process Reengineering
- Requirements Definition
- Project Plan Development
- Technology Planning and Assessment
- IT Strategic Planning
- Policy and Procedure Development
- Operational Assessment
- Digital Government
- IT Best Practices
- Project Management Office
- Business Intelligence
- Information Exchange
- RFP Development
- Quality Assurance
- Systems Integration
- Systems Architecture
- COTS Implementation



Michael Stein

Page 2



Skills

- **Areas of Expertise**
 - Project Management
 - IT Governance
 - Needs and Gap Analysis
 - Business Process Re-Engineering
 - Requirements Definition
 - Project Plan Development
- **Technology Planning & Assessments**
 - Technology Planning and Assessments
 - Strategic Planning
 - Policy and Procedure Development
 - Operational Assessments
 - Digital Government
 - IT Best Practices
 - Project Management Office
- **Other Technical Areas**
 - Business Intelligence
 - Information Exchange
 - RFP Development
 - Quality Assurance
 - Systems Integration
 - Systems Architecture
- **Certifications**
 - Information Technology Strategic Planning
 - Project Management
 - Total Quality Management



Brian Ganley
Senior Project Consultant



Experience Summary

Senior IT and public sector technology executive with more than 25 years of experience leading application, infrastructure, communications, and enterprise technology functions for municipal and county organizations. Brings deep expertise in strategic planning, large-scale project delivery, cybersecurity and disaster recovery planning, infrastructure modernization, budget and vendor management, and stakeholder engagement across executive leadership, elected officials, public safety, utilities, and regional partners. Recognized for building service-oriented teams, strengthening governance and security posture, and delivering practical, business-aligned technology solutions that improve operations, resilience, and customer service.



Professional Experience

SDI Presence LLC

(10/2023 - Present)

Senior Project Consultant

- Delivered IT infrastructure assessments, business impact analysis workshops, and continuity planning for public sector and utility clients.
- Supported development of IT strategic planning initiatives, including assessment of current IT operations and strategic roadmap development for Rancho California Water District.
- Prepared cybersecurity and resiliency deliverables, including incident response, disaster recovery, and business continuity plans for clients including Helix Water District, Elsinore Valley Municipal Water District, and City of Vista.
- Assessed City of Manteca's readiness for the MISAC Excellence Award application.

City of Manhattan Beach

(12/2020 - Present)

IT Project Manager

- Managed complex IT initiatives as a part-time retired annuitant, providing project leadership across infrastructure, resilience, and enterprise technology efforts.
- Led IT infrastructure assessment and recommendations, disaster recovery and business continuity planning, and citywide and regional fiber documentation and planning.
- Directed core switch planning, procurement, and implementation, along with storage area network procurement and deployment.
- Supported Microsoft 365 licensing, enterprise agreement renewal, and implementation, and oversaw deployment of Arctic Wolf network monitoring and SIEM capabilities.



AREAS OF EXPERTISE

- IT Leadership
- Application and Infrastructure Management
- IT Strategic Planning
- IT Assessments
- Disaster Recovery Planning
- Business Continuity Planning
- Cybersecurity Incident Response Planning
- Business Impact Analysis
- Large-Scale Project Management
- IT Operations Management
- Public Sector Technology Management
- Budget Development and Management
- Contract Negotiation and Management
- Team Leadership and Development
- Stakeholder Engagement
- Customer Service Improvement
- Process Improvement
- Technology Governance
- Infrastructure Modernization
- Communications and Radio Systems Management

SKILLS

- Infrastructure & Operations
- Cybersecurity, Resilience & Continuity
- Applications & Business Systems
- Communications & Public Safety Technology
- Project & Vendor Management
- Tools & Platforms
 - Arctic Wolf
 - Office 365
 - Microsoft 365
 - Microsoft Azure Government Cloud
 - SIEM



County of Ventura

(07/2018 - 07/2020)

Chief Information Officer

- Led the Information Technology Services Department with a staff of 180, supporting nearly 9,000 users, desktops, applications, and communications systems across County operations.
- Oversaw technical services, network, and applications divisions supporting major departments including Sheriff, Fire, Library, and Healthcare.
- Improved customer service processes, procedures, and performance, including implementation of regular customer service meetings with departments and stakeholders.
- Managed the public safety radio system and participated in regional fiber and broadband initiatives.
- Standardized and strengthened security for desktops, mobile platforms, and cloud-based applications.
- Supported modernization initiatives including transition from analog telephony to voice over IP and ongoing support for mobile phones and devices.

Los Angeles Police Department

(10/2017 - 07/2018)

Chief Information Officer

- Led the Information Technology Bureau with a staff of 180, supporting 13,500 users, 8,000 desktops, and an approximately \$34 million budget excluding personnel.
- Managed infrastructure, security, application development, and radio systems for a large public safety organization.
- Presented technology strategy and program updates to executives, stakeholders, City Council, and various Commissions.
- Established a customer service and change management philosophy for the Bureau and maintained ongoing "Top 10" project management and strategic plan updates.
- Directed implementation of Office 365 and Azure Government cloud services.
- Oversaw deployment of body-worn cameras, in-car video systems, and replacement of 11,500 portable and 4,500 mobile radios.
- Managed support for approximately 10,000 mobile phones and devices and prepared the organization for Windows 10 deployment and virtual desktop implementation.
- Directed the records management system upgrade.

City of Glendale

(05/2013 - 10/2017)

Chief Information Officer

- Directed all technology functions for the City, overseeing Infrastructure, Applications, and Wireless Communications divisions, with a staff of 49 and an annual budget of approximately \$19 million.
- Supported 2,200 desktops and users across 14 departments, including Police, Fire, Library, and utility operations.



Education

California State University, Northridge / 2001

Master of Public Administration

University of Southern California / 1990

Bachelor of Science in Business Administration



Christopher Benson
Senior Project Consultant



Experience Summary

Senior Project Consultant and accomplished IT executive with more than 36 years of experience leading municipal technology organizations, infrastructure modernization, and enterprise systems support. Brings deep expertise in IT strategy, public sector operations, telecommunications, public safety technology, and organizational change, with a strong record of guiding mission-critical implementations, rebuilding trust in IT functions, and aligning technology investments with business and service objectives. Recognized for decisive leadership, strategic planning, stakeholder partnership, budget oversight, and the delivery of reliable, cost-effective technology solutions across complex enterprise environments.



Professional Experience

City of Redondo Beach

(04/2000 - 03/2023)

Information Technology Director

- Directed citywide information technology strategy, infrastructure, and operations across all departments, including public safety and telecommunications.
- Led enterprise-wide, mission-critical technology projects and major upgrades across telecommunications, networks, personal computing, email, printing, servers, virtualization, storage, and software platforms.
- Partnered with City leadership and department stakeholders to develop strategic, cost-effective technology solutions, address organizational gaps, and maintain trusted vendor relationships.
- Managed the transition of the Information Systems Division to an IT Department and rebuilt the department's reputation and organizational trust over a multi-year period.
- Served on the Executive Steering Committee with accountability for transitioning from an in-house legacy financial and payroll system to a vendor-supported Tier II ERP, including ongoing oversight and support.
- Contributed as a member of the Department Head Executive Team in weekly leadership meetings and biannual strategic planning sessions with elected officials.
- Developed and enforced City information technology policies and procedures and prepared the annual IT budget.
- Oversaw public safety technology infrastructure, including the 911 call center, mobile data computers, and the on-premise records management system, while providing 24x7x365 support for critical City and Police Department systems.
- Established an ongoing IT equipment replacement program and led the transition from an in-house PC maintenance model to a vendor-supported service model.
- Built a redundant private fiber network connecting 12 offsite City facilities to the City Hall data center.
- Successfully supported five City Managers over a 23-year tenure.

AREAS OF EXPERTISE

- IT Infrastructure Management
- IT Strategy and Planning
- Technology Leadership
- Enterprise Systems Implementation
- Public Sector Information Technology
- Public Safety Technology Systems
- Telecommunications Management
- Network Infrastructure
- Server, Storage, and Virtual Infrastructure
- ERP Implementation and Oversight
- IT Operations Management
- IT Policy and Procedure Development
- IT Budget Development and Management
- Vendor Management
- Cross-Functional Stakeholder Engagement
- Organizational Change Leadership
- IT Service Restoration and Trust Rebuilding
- Mission-Critical Systems Support
- Technology Modernization
- Systems Administration

CERTIFICATIONS

- Novel Engineer



City of Redondo Beach

(01/1997 - 04/2000)

Information Systems Manager

- Assumed permanent management of the revamped IT Division within the Administrative Services Department, with responsibility for the City's overall technology infrastructure.
- Restored IT staffing levels, rebuilt internal department relationships, and reestablished confidence in the IT function during executive management turnover.
- Developed the budget for the reorganized Information Technology Division and initiated strategic planning for future technology changes.
- Implemented the City's first citywide PC deployment and replacement of dumb terminals.
- Began the transition away from in-house legacy financial and payroll systems.
- Directed all Y2K-related technology modifications, updates, and full system replacements.
- Programmed Y2K workarounds for legacy financial, payroll, building permit, and related systems.

City of Redondo Beach

(01/1995 - 01/1997)

Senior Programmer Analyst

- Expanded development and system administration responsibilities for the public safety system and physical technology infrastructure.
- Supported the City's transition from peer-to-peer networking and helped implement its first Ethernet network.
- Increased collaboration with multiple departments and worked directly with department directors on technology needs.
- Assumed temporary management responsibility for the Information Systems Department during a period of organizational disruption.
- Coded electronic direct deposit functionality into the in-house payroll system.
- Transitioned payroll check printing from dot-matrix to laser printing.
- Developed customized input screens for public safety system queries across local, County, and State databases.



Education

California State University / 1987

Bachelor of Science – Business Administration, Computer Methods & Administrative Systems



Skills

- **Infrastructure & Platforms**
- **Systems Administration & Operations**
- **Applications & Enterprise Systems**
- **Programming & Development**
- **IT Leadership & Governance**
- **Security**



Schermer Garrick
Data Strategy Consultant



 Experience Summary

Accomplished data and analytics leader with over 25 years of experience delivering enterprise data platforms, analytics solutions, and product strategies across public sector and global commercial environments. Brings deep expertise in data strategy, architecture, integration, governance, AI and advanced analytics, with a strong track record of leading technical teams, advising business and executive stakeholders, and aligning technology roadmaps to operational and strategic objectives. Recognized for driving scalable, data-driven solutions that improve reporting capabilities, strengthen governance and security, enable product innovation, and deliver measurable business value.

 Professional Experience

City of Sunnyvale: Data Strategy

(03/2026 - Current)

Data Strategy Consultant

- Assessing and implementing M365/Copilot security audit and implementation activities for the City of Sunnyvale.

City of Sacramento: Data Strategy

(08/2025 - 12/2026)

Data Strategy Consultant

- Conducted a comprehensive data governance assessment using SDI's Data Governance Maturity Model, tailored for public sector requirements.
- Determined current data governance maturity levels across organizational domains and identified gaps in enterprise vision, policies, responsibilities, and tools.
- Addressed immediate challenges including lack of standardization, limited real-time data access, and insufficient documentation.
- Delivered quick wins through development of foundational policies, procedures, and standards.
- Developed a long-term strategic vision for data governance, architecture, and organizational maturity.
- Promoted adoption of best practices to strengthen a data-driven culture across departments.

Virtuous Software: Analytics & Insights

(11/2024 - 05/2025)

Senior Technical Product Manager

- Led product strategy and vision for Analytics and Insights offerings.
- Provided technical leadership, including team development and mentoring, while partnering with business stakeholders.

AREAS OF EXPERTISE

- Enterprise Data Strategy
- Data Architecture
- Data Integration
- Data Governance
- Data Security
- AI and Advanced Analytics
- Data Platform Architecture
- Azure Data Platforms
- Snowflake
- AWS Data Platforms
- Azure Databricks
- ETL Strategy
- API Strategy
- Data Modeling
- Analytics Product Strategy
- Technical Product Management
- Data Engineering Leadership
- Business Intelligence Leadership
- Digital Transformation
- Executive Stakeholder Communication

CERTIFICATIONS

- ITIL v3 Foundation
- Snowflake SnowPro Core

SKILLS

- Data Strategy & Governance
- Cloud & Data Platforms
- AI & Analytics
- Programming & Tools
 - Python
 - Google Assistant



RSM US: Data & Analytics

(01/2022 - 10/2024)

Platform Director, Director of Data Engineering

- Led the Azure-based Enterprise Data Platform, ensuring functionality and availability to support enterprise reporting and analytics.
- Partnered with business leadership to define priorities and reporting capabilities aligned to firmwide objectives.
- Drove innovation in data processing and data quality to improve enterprise decision support.
- Defined and enforced data governance and data security policies for the enterprise reporting environment.
- Created and maintained the technology roadmap, aligning platform investments with overall firm strategy.
- Led and mentored Data Engineering and Business Intelligence teams to deliver scalable, high-quality technology solutions.
- Reduced Azure run costs by \$2M annually through analysis and optimization of compute and storage consumption.
- Supported development of the modern data platform leveraging Azure and Databricks.

PPG Industries: Digital Transformation

(03/2021 - 01/2022)

Data Transformation Consultant

- Supported delivery and execution of AI and machine learning applications tied to strategic initiatives.
- Contributed to efforts to reduce manufacturing costs, improve production quality, and lower energy consumption.
- Supported build and deployment of AI/ML solutions while advancing digital solution adoption and implementation best practices.
- Drove process changes to improve operational effectiveness in digital transformation initiatives.

Octopi Commerce: AI Product Development

(01/2019 - 01/2021)

AI Product Director

- Directed product development strategy, market feedback integration, and product enhancement for a multi-Point of Sale partner integrated application.
- Led design, delivery, and implementation of a data platform supporting machine learning and AI-driven merchant applications.
- Delivered the initial product offering integrating merchant Point of Sale platforms with the REACH product portal to improve scheduling efficiency and customer targeting.
- Architected the application data model to standardize data across multiple Point of Sale partners for internal AI analysis.
- Managed Azure SQL and Data Lake architecture, including API-based data integration.
- Created the data model for the OLTP scheduling application in Azure SQL and Azure Data Lake.
- Architected the AI/ML layer in Azure Databricks and managed end-to-end data flow from Point of Sale partners through the transactional and analytics layers.



Education

University of Chicago

Master of Arts, International Relations

Northwestern University

Bachelor of Arts, Political Science & International Studies

EXHIBIT “2”
TO
TASK ORDER NO. 1
COMPENSATION



Cost Proposal Prepared For:

West Valley Water District

IT Master Plan
RFP #2026-06

July 30, 2026



Respectfully Submitted By:



Patrick Griffin
Managing Director
pgriffin@sdipresence.com
714-975-4150

SDI developed its project costs based on our extensive experience completing similar projects, along with our research on the District's organization, size, and structure. We propose completing the District's project utilizing a total of 475 hours at a total cost of \$115,960. Detailed information about the number of hours, along with cost by Phase and Task are presented in the table below.

Task Descriptions	Hours	Cost
Phase 1 - Initiate		
1.1 Facilitate Project Planning Meeting	4	\$ 1,020
1.2 Work Plan Development and Review	3	\$ 760
1.3 Request Existing Documentation	12	\$ 2,940
1.4 Conduct Project Kickoff Meeting	6	\$ 1,480
Subtotal: Phase 1 - Initiate	25	\$ 6,200
Phase 2 - Assess		
2.1 Conduct "Voice of the User" Survey	40	\$ 9,640
2.2 Conduct Business Applications Assessment	120	\$ 29,100
2.3 Perform IT Assessment	130	\$ 31,900
2.4 Conduct Management Briefing	8	\$ 2,020
2.5 Develop and Deliver IT Assessment Report	60	\$ 14,600
Subtotal: Phase 2 - Assess	358	\$ 87,260
Phase 3 - Deliver		
3.1 Develop IT Project Portfolio	12	\$ 2,940
3.2 Conduct Project Prioritization Workshop	20	\$ 4,960
3.3 Prepare IT Master Plan	60	\$ 14,600
Subtotal: Phase 3 - Deliver	92	\$ 22,500
Total	475	\$ 115,960

SDI's hourly rates and budgeted labor hours for our consultant team are as follows:

SDI Resource	Hourly Rate	Budgeted Labor Hours
Patrick Griffin – Delivery Executive	\$260	10
Lee Curtis – Project Manager	\$250	126
Mike Stein – Project Consultant	\$240	111
Brian Ganley – Project Consultant	\$240	125
Chris Benson – Project Consultant	\$240	53
Garrick Schermer – Project Consultant	\$250	50

Hourly rates include all associated project-related expenses including travel. Please note that SDI does **not** charge its clients for consultant travel time.

SDI typically invoices its clients monthly for work performed in the prior month. Invoices are substantiated by detailed descriptions of tasks performed by SDI resources, and number of hours to complete the task. SDI is open to discussing other methods for invoicing during the project, including for example a deliverables-based milestone billing structure.

EXHIBIT “3”
TO
TASK ORDER NO. 1
SCHEDULE

Name of Organization	Helix Water District	
Address	7811 University Avenue La Mesa, CA 91942	
Name of Contact	Jennifer Bryant, Director of Administrative Services	
Telephone and Email	(619) 667-6259 Jennifer.bryant@helixwater.org	
SDI Resources Assigned	Patrick Griffin – Delivery Executive Lee Curtis – Project Manager Brian Ganley – Project Consultant	
Completion Date & Cost	October 2022 \$91,908	
IT Assessment & IT Strategic Plan SDI completed an IT assessment of the organization’s technology operations and assisted with the development of a comprehensive IT Strategic Plan. Subsequent to completion of the Plan, SDI was contracted to develop a Disaster Recovery / Business Continuity Plan and also conducted a presentation on AI to the District Board of Directors.		

Name of Organization	Central Contra Costa Sanitary District	
Address	5019 Imhoff Place Martinez, CA 94553	
Name of Contact	Charles Mallory, CIO	
Telephone and Email	(925) 566-4589 cmallory@centralsan.org	
SDI Resources Assigned	Patrick Griffin – Delivery Executive Lee Curtis – Project Manager Mike Stein – Project Consultant	
Completion Date & Cost	October 2023 \$430,080	
IT Assessment & IT/OT Strategic Plan SDI partnered with Brown & Caldwell to complete a comprehensive assessment of the District’s technology operations and service delivery for the entire organization, and provided recommendations designed to improve overall technology service delivery for the organization. SDI also developed a technology acquisition roadmap and incorporated the entire project into an IT Strategic Plan which is being utilized by the District to guide future technology investments. SDI recently completed an assessment of the District’s permitting system and is currently assisting with the acquisition of a replacement system.		

Section II Methodology and Approach

The District seeks to partner with a consulting company that has vision and leadership in IT master planning. SDI brings the District the experience, expertise, and proven methods to help ensure project success. SDI has developed a comprehensive methodology designed specifically to meet the unique needs of organizations seeking to develop strategic technology plans. This methodology is based on our hands-on experience in working with public sector clients, and it continues to evolve as new best practices are identified.

SDI's approach to IT strategic planning is designed specifically to meet the needs of organizations seeking to develop an integrated IT Master Plan that can be used to guide technology initiatives for the next three to five years. It is important to note that the cornerstone of our approach is the focus and emphasis on the involvement and interaction with the department consumers of technology and those setting the business direction for the District – providing a voice of the IT customer to the resulting Information Technology Master Plan. The team will seek and incorporate input from all departmental technology consumers and stakeholders in the District's operating departments and divisions. Our approach includes three distinct phases:



SDI believes that a critical component of this project is to ensure that the stakeholders and staff impacted understand the trade-offs, resources, risks, and timelines associated with the project approach, and have appropriate expectations prior to, and throughout, the project life cycle. To accomplish this, SDI's approach includes the following guiding principles:

- Focus on an open and collaborative process that encourages a consensus among the participants and a shared commitment to the successful completion of a comprehensive IT Master Plan
- Use a structured, proven approach to ensure comprehensive understanding of requirements and business needs at all levels of the District
- Strive to minimize disruption to daily District operations throughout the various processes by ensuring a well planned and executed project
- Fully identify and disclose the potential opportunities as well as the risks involved and provide realistic risk management and mitigation strategies
- Ensure that stakeholders and users have and maintain realistic expectations throughout the process

Figure 1 on the following page identifies the phases, tasks, and deliverables for this project.



Figure 1 – Project Approach and Deliverables

SDI understands that the District is interested in having an information technology consultant develop an IT Master Plan to guide it in the effective planning, procurement, implementation, and management of technology. SDI’s approach to ITMP development entails several critical milestones during the overall process, and SDI provides specific deliverables throughout the project. SDI recognizes and is prepared to address the following key considerations for the ITMP:

- Completion of a comprehensive assessment of existing technology and associated IT support environment
- Development of a comprehensive ITMP that aligns overall District technology resources with the objectives of the user departments and overarching organizational objectives. This includes recommended projects, their respective implementation priority, cost estimates for each project, and an implementation strategy that can be incorporated into the District’s annual budget process
- Recommendations for new and emerging technologies that may help improve the efficiency and effectiveness of the District’s IT service delivery

SDI’s IT planning methodology is built on our experience in delivering services to California local government agencies for over 30 years. After the completion of each project, we sit down to determine what we can change to make the next plan we develop even better. This has benefited our clients by establishing a methodology that is proven and continues to evolve to meet the unique and changing needs of our public sector clients.

A cornerstone of SDI’s methodology is the focus and emphasis on the involvement and interaction with the department users of technology and those setting the business direction for the District – providing a “voice of the customer” to the resulting ITMP. SDI will incorporate input from all users and stakeholders, up to and including the District’s elected officials (if desired), Executive Management, and the operating departments and divisions.

SDI is familiar with the challenges and issues that can arise in developing such plans. For example, we are skilled in managing multiple, and often conflicting, stakeholder visions, missions, goals, objectives, needs, and priorities. In addition, we are sensitive to the desires of elected and appointed officials and the public for transparency and open government. Our proposed methodology carefully considers project prioritization and includes processes to help manage competing priorities to ensure the ITMP provides a true District-wide perspective. We pride ourselves in helping organizations develop plans that are realistic and attainable in terms of available budget, resources and time.

On the following pages, we describe in further detail each of the three Phases of the IT Assessment and Master Plan process, along with a recommended approach for the ongoing IT Governance oversight for the Plan.

Phase 1 - Initiate

As project management professionals, SDI recognizes the importance of applying a formal project management framework to this project to ensure that it meets objectives and is delivered on- time and on-budget. The purpose of the Initiate Phase is to prepare for, and initiate, the project under a well-defined work plan. This phase includes confirming our understanding, as well as the understanding of the stakeholders, regarding the scope of work and the process for accomplishing the overall objectives of the project. Table 2 provides a detailed discussion of what each task in the Initiate phase entails.

Table 2 – Initiate Phase Tasks and Deliverables

Project Approach: Phases and Tasks		Deliverables
Phase 1 Initiate	1.1 – Facilitate Planning Meeting 1.2 – Work Plan Development and Review 1.3 – Request Existing IT Documentation 1.4 – Conduct Kickoff Meeting	✓ Project Work Plan ✓ Documents Request ✓ Kickoff Meeting Presentation
1.1 – Facilitate Planning Meeting		
TASK DESCRIPTION: SDI will meet with the District’s Project Sponsor to complete a detailed review of the scope of work, project timeline, deliverables, project status methods, project participants (i.e. sponsor, subject matter experts, technical resources, etc.), and other items to ensure a well-planned project. During this meeting, SDI will discuss the tools and templates that will be leveraged.		
1.2 – Work Plan Development and Review		
TASK DESCRIPTION: SDI will publish a Work Plan and facilitate a meeting with the District Project Sponsor to review and obtain feedback on the proposed Work Plan. The goal of this meeting is to obtain consensus on the Work Plan and a commitment to support the Work Plan. The Work Plan will be continuously updated throughout the project timeline as part of regular status reporting.		
DELIVERABLES: Draft and Final Work Plan		

1.3 – Request Existing IT Documentation

TASK DESCRIPTION: To support the activities associated with Phase 2 of the project, SDI will request and review documentation including, but not limited to, the following:

- District Goals
- District Strategic Business Plan, Budget, and CIP
- Previous Related Assessments and Plans
- District Organizational Chart and Contact Information
- Technology Budgets and Capital Plans
- Technology Governance Agendas and Minutes
- In Process or Planned Technology Project Documentation
- IT Inventory
- IT Policies and Procedures
- IT Disaster Recovery Plan
- Network Architecture Documentation
- IT Service Level Agreements
- IT Performance Statistics or Activity Reports
- Technology Vendor Listing and Agreements

DELIVERABLE: Documents Request

1.4 - Conduct Kickoff Meeting

TASK DESCRIPTION: Since the project will have an enterprise-wide impact, it is important to proactively communicate with all impacted staff to ensure a clear understanding of project goals and objectives, roles and responsibilities, approach, tasks, and timeline. The Kickoff Meeting also provides the opportunity to introduce the SDI team to District staff and should involve senior level management and project sponsors to provide introduction of this District-wide endeavor. It is important that all District staff that will be involved in the project, regardless of their role, participate in the Project Kickoff meeting.

DELIVERABLE: Kickoff Meeting Presentation

Phase 2 - Analyze

In developing the ITMP, it is necessary to first have a comprehensive and realistic understanding of how effectively the current IT organization and assets meet the District’s requirements, the District’s business objectives and priorities, and how the District desires to use technology as a key enabler in supporting its business in the future. This “look ahead” must take into account that not only is technology evolving rapidly, but so are public expectations regarding timely and easy access to District services and information transparency. In the Analyze Phase, SDI’s consultants work closely with District technology stakeholders to define the future vision for the District’s use of technology and the gap between that vision and the District’s current IT infrastructure. SDI’s consultants will develop an assessment as to how well the District’s IT services comply with best practices and will identify gaps between the level of service provided by the District’s IT resources and user service level expectations.

The IT Assessment is developed based on information gathered through in-person interviews, the results of an easy-to-use, online survey that is available to all District users, interviews with IT personnel, site visits, an assessment of the degree to which the District and its IT organization conform to information technology best practices, and a review of the District’s technical documentation.

In those areas where the Assessment indicates that action is needed, SDI will provide a finding and one or more recommended actions, an assessment as to the relative priority of each recommendation, and an action plan that considers the relative importance of each recommendation along with a timeframe for implementation. Table 3 describes in detail the activities associated with the Analyze phase.

Table 3 – Analyze Phase Tasks and Deliverables

Project Approach: Phases and Tasks		Deliverables
Phase 2 Analyze	2.1 – Conduct “Voice of the User” Survey	✓ “Voice of the User” Survey
	2.2 – Conduct Business Technology Assessment	✓ Draft and Final Survey Reports
	2.3 – Perform IT Assessment	✓ Verbal Briefing of IT Assessment Findings
	2.4 – Conduct Management Briefing	✓ Draft and Final IT Assessment Report
	2.5 – Develop and Deliver IT Assessment Report	
2.1 – Conduct “Voice of the User” Survey		
TASK DESCRIPTION: SDI will conduct a web-based user survey to determine overall satisfaction in terms of IT service delivery and support. The survey will be available to all District technology users and provides an opportunity to obtain their input. Once the survey is concluded, SDI will prepare a Survey Results Report. The report will summarize the survey results and present best practices targets for each survey question. The best practices targets represent what a well-funded and high performing IT service delivery organization would strive to attain. The information gathered from the online survey provides valuable input to the IT Assessment.		
DELIVERABLES: “Voice of the User” Survey, Draft and Final Survey Reports		
2.2 – Conduct Business Technology Assessment		
TASK DESCRIPTION: SDI will facilitate a series of workshops with District departments to identify the current technology environment within each organization, barriers to full utilization of those technologies, and planned uses and expansion of technology in the future. The workshops will be held for each department and attended by department managers and key staff as directed by the District. As part of this activity, SDI will create an Application Effectiveness Matrix that evaluates how key applications are used by the departments to fit their current and future needs.		

2.3 – Perform IT Assessment

TASK DESCRIPTION: SDI's IT Assessment evaluates whether the District's IT infrastructure and support organization are prepared to support the future needs of the District by reviewing six key operational "assessment dimensions." This review takes a comprehensive **best practices** view of essential IT delivery components, as a weakness in any one particular dimension can adversely influence the overall effectiveness of the organization. Findings and recommendations are developed based on:

- Information gathered in the course of the business technology interviews with department stakeholders
- The results of the Voice of the User Survey
- Interviews with IT managers and staff
- The IT best practices assessment

SDI's team will consolidate this information and develop findings and recommendations based on the District's compliance with best practices in the following dimensions:

- **Technology Governance** – Evaluation of the current IT organization and assessment of its skills, staffing levels, and capability to support operation and maintenance of current and future systems. This will include a review of IT project management practices, planning activities, IT refreshment, and the use of oversight committees.
- **Service Delivery** – Evaluation of the daily operation of the IT environment including budget, service metrics, maintenance, help desk, configuration management, change management and capacity management.
- **Business Technology Applications** – Evaluation of the processes and methods to support business and operational applications.
- **Data Management** – Analysis of data management practices and governance, data integration opportunities, and potential business intelligence (BI) applicability.
- **Security** – Evaluation of the use of software monitoring tools, virus protection procedures, physical hardware security, network vulnerability, passwords, data backup/recovery processes, physical and data security, integrity planning, PCs, network, firewall, incident response, patch management, anti-virus protection and emergency operations.
- **Infrastructure** – Review of the network, servers, desktops, telephony, storage configurations, remote access, data storage, server management, and operational procedures.
- **Administration** – Review of technology procurement processes, contract management, vendor management, software license management, budget/charge back management and physical inventory processes.

2.4 – Conduct Management Briefing

TASK DESCRIPTION: Upon compilation of the initial findings and recommendations from the IT Assessment activities, SDI will meet with the District’s Project Sponsor to review and discuss these items prior to the development of the draft IT Assessment Report.

DELIVERABLE: Verbal Briefing of IT Assessment Findings

2.5 – Develop and Deliver IT Assessment Report

TASK DESCRIPTION: After reviewing initial findings and recommendations with the District’s Project Sponsor, SDI will prepare a draft IT Assessment Report and review it with the District’s key stakeholders. Following the review, SDI will incorporate revisions as needed and deliver a Final Report. The completed IT Assessment Report will include a summary of the user survey, a summary of the best practices assessment, a SWOT (strength, weaknesses, opportunities, and threats) analysis, specific findings and recommendations that are realistic and actionable, and a proposed action plan for their implementation.

DELIVERABLES: Draft and Final IT Assessment Report

Phase 3 – Strategize

In Phase 3 – Strategize, SDI works with the District to review and analyze the findings of previous phases in order to identify, analyze, and prioritize projects that need to be included in the ITMP. SDI brings to the District proven methods and tools to ensure identified projects are well defined, understood by the stakeholders, and prioritized using agreed upon criteria. During this task, SDI will facilitate a Project Prioritization Workshop that uses a multi-step process to arrive at a District-wide prioritization of identified projects that will provide the basis for a roadmap in the ITMP. Table 4 provides detail regarding the Strategize phase of the process.

Table 4 – Strategize Phase Tasks and Deliverables

Project Approach: Phases and Tasks		Deliverables
Phase 3 Strategize	3.1 – Prepare for Prioritization Workshop	✓ IT Project Portfolio ✓ Prioritization Workshop Materials ✓ Draft and Final IT Master Plan
	3.2 – Conduct District-Wide Prioritization Workshop	
	3.3 – Prepare IT Master Plan	
3.1 – Prepare for Prioritization Workshop		
TASK DESCRIPTION: SDI will utilize the results of the IT Assessment Report to identify projects that will improve the District’s current use of technology and serve the District’s longer-term technology needs. The output of this effort will be an IT Project Portfolio that identifies recommended projects, and provides additional information for each of the projects including the project’s sponsor(s) and other impacted departments, a project description, cost estimates, assessment of the level of effort and the level of risk involved in the implementation of the project, an assessment of the potential business impact, and other criteria to prepare stakeholders for the Planning and Prioritization Workshop.		
DELIVERABLE: IT Project Portfolio		

3.2 – Conduct District-Wide Prioritization Workshop

TASK DESCRIPTION: SDI believes we have many unique and proven methods to develop a successful ITMP; however, this activity alone sets us apart from all our competitors. SDI encourages the District to call our references and inquire about our innovative “Blue Wall Prioritization Workshop” approach that drives enterprise-wide consensus and acceptance of the IT Master Plan.

Our Blue Wall approach uses a multi-step prioritization methodology and tools that encourages staff participation and collaboration. The workshop is designed to help drive consensus to obtain District- wide prioritization of projects. The end result of the workshop will be a prioritized list of projects assigned to implementation timeframes. In addition, the workshop is designed to identify ITMP enabling factors which are defined as key elements that must be in place or occur to allow the Plan to be a success. Examples of enabling factors could include training, staffing, budget, governance, project management, and change management.

DELIVERABLES: Prioritization Workshop Materials

3.3 – Prepare IT Master Plan

TASK DESCRIPTION: SDI will incorporate work products from previous tasks as the foundation for the development of the District’s Information Technology Master Plan. SDI will use this information, as well as other information provided by staff and independent research to create a draft of the ITMP and review it with the District. The ITMP will provide a summary of the requirements that drove the need for the plan, review key information technology trends that will impact the District, and review the results of the Planning and Prioritization Workshop and the subsequent review and refinement of the project roadmap from the workshop.

SDI will revise and update the ITMP based on feedback from the District and will conduct a final technical and quality review of the final ITMP before submission to the District’s management team.

DELIVERABLES: Draft and Final Information Technology Master Plan

Project Timeline

Based on SDI's experience with similar projects, as well as our knowledge of the District's environment, we estimate that this project will require approximately 16 weeks to complete. Figure 2 below identifies the estimated weeks per phase.

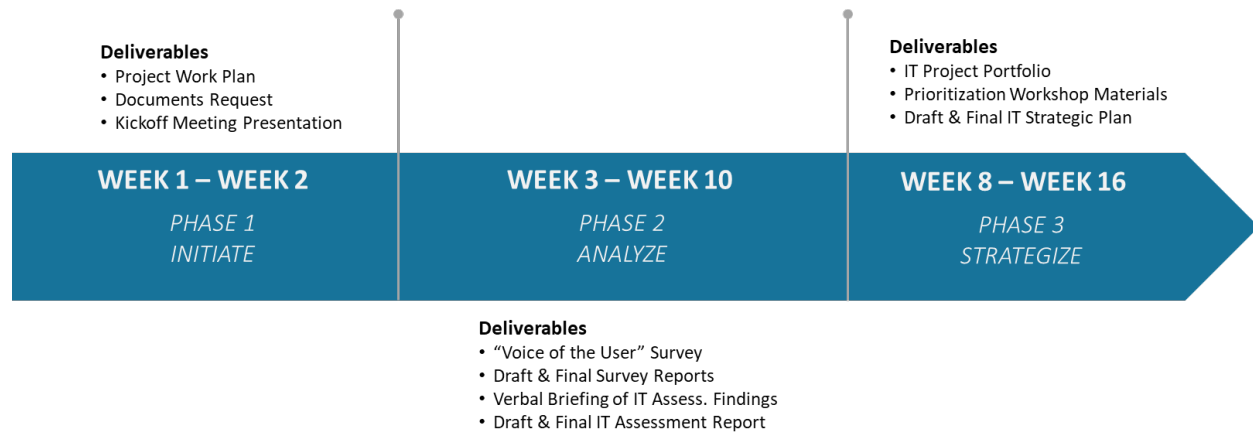


FIGURE 2 – PROJECT SCHEDULE

The success of achieving this schedule largely depends on the availability of the District's assigned staff, along with the timely completion of tasks required of District personnel including reviewing draft documents and scheduling of staff for required meetings.

EXHIBIT B
KEY PERSONNEL

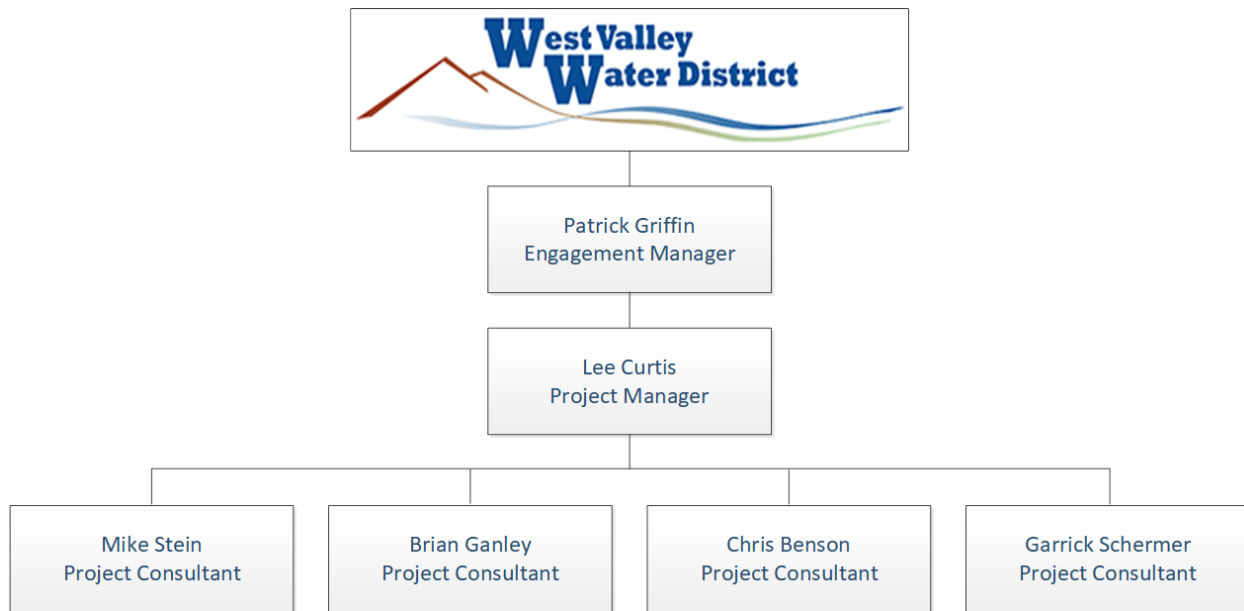


Figure 4 - Project Team

Patrick Griffin – Engagement Manager

Role: Mr. Griffin will serve as the Engagement Manager on the District’s project, bringing his years of experience working with public agencies to support the District and the project team on this important project. Mr. Griffin will provide management oversight and support to the SDI project team, interacting with the District team on contractual and business-related matters.

Biography: Mr. Griffin has over 40 years of experience in California local government. His municipal experience includes serving in various positions, including Controller, Finance Director, Community Development Director, and Assistant City Manager, with the latter position involving responsibility for the city-wide budget, information technology, and public communications and outreach. After retiring from the public sector in 2012, Mr. Griffin began a consulting career with NexLevel Information Technology, which merged with SDI in 2017. During his consulting career, Mr. Griffin has been responsible for completing dozens of IT Strategic Plans, as well as ERP and land management system procurements and implementations for local agencies.

Lee Curtis – Strategic Planning Practice Lead and Project Manager

Role: Mr. Curtis will serve as the project manager for the engagement, overseeing day-to-day project activities.

Biography: Mr. Curtis is a senior-level, hands-on executive with more than 40 years of experience in technology service and management consulting. He has been a top-tier manager with outstanding technology delivery skills and expertise in long-range project planning. Mr. Curtis has provided executive-level consulting to both the private and public sectors, supporting a wide range of technology implementations. With over 25 years at SDI, he is an experienced project manager, accomplished writer, and a well-versed consultant providing in-depth technology assessments and innovative strategic plans to public sector clients. Mr. Curtis has served as CIO or IT Director for numerous organizations across the country. He has presented IT Strategic Planning sessions at the Municipal Information Systems Association of California (MISAC) annual conferences. In 2020, he

presented a webinar on Strategic Planning to the Association of California Water Agencies (ACWA). Mr. Curtis has participated in assessments and planning projects for numerous cities, counties, and special districts.

Mike Stein – Project Consultant

Role: Mr. Stein will provide subject matter expertise throughout the project and will take a lead role in developing draft project deliverables.

Biography: Mr. Stein is a highly experienced management and technology consultant with more than four decades of experience in the public sector, the telecommunications industry and commercial banking. His career has been focused on helping organizations implement complex technology solutions and effectively utilize technology to solve business problems through business process re-engineering, IT strategic planning, procurement assistance, definition of requirements, and project management. Mr. Stein has been a key member of the project team for numerous strategic planning efforts since joining SDI in 2013.

Brian Ganley – Project Consultant

Role: Mr. Ganley will be SDI's Subject Matter Expert and will be responsible for performing tasks associated with the project, including the project deliverables. Mr. Ganley will provide focused technical expertise throughout the project, emphasizing critical components of the IT organization's operations, IT Service Delivery, IT infrastructure, applications, and cybersecurity.

Biography: Mr. Ganley is an experienced public sector information technology leader focusing on customer service, collaboration with stakeholders, strategic planning, and innovative technology solutions. Mr. Ganley is a hands-on technologist with extensive experience in cybersecurity, networking, and infrastructure, as well as a strong technical background. He was the Chief Information Officer for the County of Ventura, where he was responsible for a technology staff of 180, supporting 9,000 users and their desktops, as well as various applications and communications systems. Prior employment included serving as the Chief Information Officer for the Los Angeles Police Department, where he led the Information Technology Bureau, comprising a staff of 180, supporting 13,500 users and 8,000 desktops, and managing a budget of approximately \$34 million. In addition, Mr. Ganley was the Chief Information Officer for the City of Glendale and the City of West Hollywood.

Chris Benson – Project Consultant

Role: Mr. Benson will provide focused expertise throughout the project, emphasizing critical components of the IT organization's operations, IT Service Delivery, IT infrastructure, and cybersecurity.

Biography: Mr. Benson is an experienced public sector information technology leader focusing on customer service, collaboration with stakeholders, strategic planning, and innovative technology solutions. Mr. Benson is a hands-on technologist with extensive experience in municipal IT, including applications, cybersecurity, networking, and infrastructure. Mr. Benson recently joined SDI after a successful career in the local government information technology field. He worked for the City of Redondo Beach in a variety of IT roles, with the last 23 years as the City's IT Director. Recently, Mr. Benson participated in the Port of Los Angeles IT Assessment and Strategic Planning project and the Stockton Port District IT Master Plan.

Garrick Schermer – Project Consultant

Role: Mr. Schermer will provide focused expertise in the area of data analysis and management.

Biography: Mr. Schermer serves as SDI's AI Data Strategy & Governance resource, leading high-impact initiatives that strengthen data governance, quality management, and analytics capabilities across public sector and enterprise clients. In this role, he has delivered major governance and data migration strategies, contributed to thought leadership in Data & AI, and developed training programs to advance organizational AI literacy. Mr. Schermer's expertise spans data strategy, governance, enterprise architecture, AI enablement, and product management, supported by deep experience with modern platforms such as Snowflake, Azure, AWS, and Databricks. He is known for building high-performing teams, mentoring technical talent, and communicating effectively with executives and stakeholders to deliver transformative results.

EXHIBIT C
INSURANCE

INSURANCE

- A. **General Requirements.** Before commencing the performance of services under this Agreement, and at all other times this Agreement is effective, Consultant must procure and maintain the following types of insurance with coverage limits complying, at a minimum, with the limits set forth below:

<u>Type of Insurance</u>	<u>Limits (combined single)</u>
Commercial General Liability:	\$1,000,000
Business Automobile Liability	\$1,000,000
Professional Liability	\$1,000,000
Workers' Compensation	Statutory Requirement

- B. **Commercial General Liability Insurance.** The amount of insurance set forth above must be a combined single limit per occurrence for bodily injury, personal injury, and property damage for the policy coverage. The insurance must be on an "occurrence" not a "claims made" basis.
- C. **Business Automobile Insurance.** Automobile coverage must be written on forms subject to the written approval of District.
- D. **Professional Liability Insurance.** This coverage must be on an "occurrence" basis, including coverage for contractual liability. The Professional Liability Insurance required by this Agreement must be endorsed to be applicable to claims based upon, arising out of or related to services performed under this Agreement.
- E. **Workers Compensation.** Consultant must have a State of California approved policy form providing the statutory benefits required by law with employer's liability limits of no less than \$1,000,000 per accident for all covered losses, or Consultant must provide evidence of an approved self-insurance program.
- F. **Additional Insureds.** Each Commercial General Liability Insurance policy and Business Auto Insurance policy must provide that the District, its officials, officers, employees, agents and volunteers are "additional insureds" under the terms of the policy and must provide that an act or omission of one the insureds will not reduce or avoid coverage to the other insureds.
- G. **Deductibles and Self-Insured Retention.** Any deductibles or self-insured retentions applicable to the insurance policies required under this Agreement must be declared to and approved by District. In no event may any required insurance policy have a deductible, self-insured retention or other similar policy provision in excess of \$50,000 without prior written approval by District in its sole discretion. At the option of District, either the insurer will reduce or eliminate such deductibles or self-insured retentions with respect to the District's additional insureds or Consultant will procure a bond guaranteeing payment of any losses, damages,

expenses, costs or settlements up to the amount of such deductibles or self-insured retentions.

- H. **Primary Insurance.** Each of the insurance policies maintained by Consultant under this Agreement must state that such insurance will be deemed “primary” so that any insurance that may be carried by District will be deemed excess to that of Consultant. This endorsement must be reflected on forms as determined by District.
- I. **Certificates of Insurance and Endorsements.** Prior to commencing any services under this Agreement, Consultant must file with the District certificates of insurance and endorsements evidencing the existence of all insurance required by this Agreement, along with such other evidence of insurance or copies of policies as may reasonably be required by District. These certificates of insurance and endorsements must be in a form approved by the Legal Counsel. Consultant must maintain current certificates and endorsements on file with District during the term of this Agreement reflecting the existence of all required insurance. Each of the certificates must expressly provide that no material change in the policy, or termination thereof, will be effective except upon 30 days’ prior written notice to District by certified mail, return receipt requested. The delivery to District of any certificates of insurance or endorsements that do not comply with the requirements of this Agreement will not waive the District’s right to require compliance.
- J. **Insurance Rating.** All insurance required to be maintained by Consultant under this Agreement must be issued by companies licensed by or admitted to conduct insurance business in the State of California by the California Department of Insurance and must have a rating of A or better and Class VII or better by the latest edition of A.M. Best’s Key Rating Guide.
- K. **Aggregate Limits.** The aggregate limits for each insurance policy required under this Agreement must apply separately and solely to the services performed under this Agreement. If the required policies do not have an endorsement providing that the aggregate limit applies separately to the services being performed, or if defense costs are included in the aggregate limit, then the required aggregate limits must be increased to an amount satisfactory to District.
- L. **Waiver of Subrogation Rights.** Consultant and each insurer providing any insurance required by this Agreement must waive all rights of subrogation against District, its officials, officers, employees, agents and volunteers, and each insurer must issue a certificate to the District evidencing this waiver of subrogation rights.
- M. **Failure to Maintain Required Insurance.** If Consultant, for any reason, fails to obtain and maintain the insurance required by this Agreement, District may obtain such coverage at Consultant’s expense and deduct the cost of such insurance from payments due to Consultant under this Agreement or may terminate the Agreement.

- N. **Effect of Coverage.** The existence of the required insurance coverage under this Agreement shall not be deemed to satisfy or limit Consultant's indemnity obligations under this Agreement. Consultant acknowledges that the insurance coverage and policy limits set forth in this Agreement constitute the minimum coverage and policy limits required. Any insurance proceeds available to District in excess of the limits and coverage required by this Agreement, and which is applicable to a given loss, must be made available to District to compensate it for such losses.