



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

**SPECIAL ENGINEERING, OPERATIONS AND PLANNING COMMITTEE MEETING
AGENDA**

Tuesday, September 1, 2026, 6:00 PM

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

BOARD OF DIRECTORS

**Director Gregory Young, Chair
Director Estevan Bennett**

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@wvwd.org.

If you require additional assistance, please contact administration@wvwd.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. Minutes of the July 23, 2026, Regular Committee Meeting
2. Updates to the Engineering, Operations and Planning Committee
3. Delegation of Limited Authority to Accept Completed District Public Works and Record Notices of Completion Pg. 5
4. Award a Construction Contract with Dominguez General Engineering, Inc. and Approve Task Order with Albert A. Webb Associates for the Bloomington Alleyway Main Replacement Phase 3B Project (W25036) Pg. 11
5. Approve Second Amendment to Reimbursement Agreement with San Bernardino Valley Municipal Water District for Hidden Valley Wetlands Mitigation Project Pg. 61
6. Resolution No. 2026-15 - Approval and Adoption of the SCADA Master Plan Pg. 69

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 agendized 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 August 27, 2026, by 6:00 p.m., in compliance with the provisions of the Brown Act.

Brandon Yoshida

Brandon Yoshida, Board Secretary

Date Posted: August 27, 2026



STAFF REPORT

DATE: September 1, 2026

TO: Engineering, Operations and Planning Committee

FROM: Rocky Welborn, Director of Engineering

SUBJECT: Delegation of Limited Authority to Accept Completed District Public Works and Record Notices of Completion

STRATEGIC GOAL:

Strategic Goal 2 - Be an Exemplary Employer; E. Cultivate an Empowering and Supportive Culture

Strategic Goal 5 – Apply Sound Planning, Innovation, and Best Practices; E. Define, Develop, and Implement Best Practices

Strategic Goal 7 – Realize Health, Safety, and Regulatory Compliance; B. Establish Compliance Programs for Staff

MEETING HISTORY:

NONE.

BACKGROUND:

A Notice of Completion (NOC) is a statutory project-closeout document that a public entity may record with the County Recorder on or within fifteen (15) days after completion of a public work of improvement. Under California Civil Code Section 9200, completion occurs at the earliest of the public entity's acceptance of the work or a continuous cessation of labor for 60 days. Civil Code Section 9204 requires compliance with the general notice-content requirements of the Civil Code.

For public works, timely recordation shortens the period for service of stop payment notices from 90 days after cessation or completion to 30 days after recordation. It affects the related deadline for actions on a payment bond. Recording an NOC therefore provides a defined closeout date for construction-claim administration and is an important risk-management tool. Acceptance and other closeout steps also support the orderly administration of retention and final payment under the contract and applicable law.

The District routinely completes capital improvement projects, facility improvements, and other public works requiring formal acceptance and closeout. Because Civil Code Section 9204 permits an NOC to be recorded only on or within fifteen (15) days after completion, the District benefits from a process that allows acceptance and recordation to occur promptly after the responsible department confirms that the work is complete and eligible for acceptance under the contract documents and applicable law.

Historically, Notices of Completion have been presented to the Board of Directors for approval before recordation. District legal counsel has advised that Civil Code Sections 9200 and 9204 do not expressly require the Board to approve the NOC itself. For purposes of the proposed process, the key governance issue is whether the person accepting the work and signing the NOC has authority to act on behalf of the District.

Legal counsel has advised that the Board may expressly delegate limited authority to District staff to accept completed District public works and execute and record NOCs. Staff therefore recommends a resolution delegating that authority to the General Manager or the General Manager's written designee, subject to documented closeout review, legal safeguards, exclusions for matters reserved to the Board, and regular reporting.

DISCUSSION:

Recording a Notice of Completion is an administrative step that follows the legally significant act of accepting completed work. Timely action is important because the NOC must be recorded on or within fifteen (15) days after completion to obtain the statutory effect of recordation.

The proposed resolution would streamline project closeout by allowing staff to act within the statutory window without waiting for a Board meeting. The delegation would apply only to District-awarded public works and construction contracts that have been authorized in accordance with District policy and for which acceptance is not otherwise reserved to the Board. It would not alter the Board's authority over contract awards, budgets, change orders, contract amendments, developer-installed facilities requiring Board acceptance, or other policy matters.

Before acceptance, the responsible department would provide a written or verbal recommendation supported by closeout documentation. The NOC would be executed and verified in a form approved by District legal counsel. Projects involving material unresolved claims or disputes, known defective work, surety issues, or other circumstances affecting the District's rights or obligations would require consultation with legal counsel before acceptance or recordation.

The General Manager intends to report actions taken under the delegation to the Board, which may include the project name, contractor, acceptance date, recordation information, approved contract amount as of acceptance, and any material outstanding claim or dispute. These controls preserve Board oversight while improving the efficiency and consistency of project closeout.

FISCAL IMPACT:

No fiscal impact is anticipated beyond routine staff time and any applicable County recording fees associated with project closeout.

REQUESTED ACTION:

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

1. Adopt Resolution No. 2026-11 delegating limited authority to the General Manager to accept completed District public works and execute and record Notices of Completion.

Attachments

[Resolution 2026-11 - Delegating Limited Authority to the General Manager to Accept Completed District Public Works and Execute.pdf](#)

RESOLUTION NO. 2026-11

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT DELEGATING LIMITED AUTHORITY TO THE GENERAL MANAGER TO ACCEPT COMPLETED DISTRICT PUBLIC WORKS AND EXECUTE AND RECORD NOTICES OF COMPLETION

WHEREAS, the West Valley Water District ("District") periodically completes District-awarded public works projects and other construction contracts requiring formal acceptance and project closeout; and

WHEREAS, California Civil Code Section 9200 provides that completion of a public work of improvement occurs at the earliest of acceptance by the public entity or a continuous cessation of labor for 60 days, and Civil Code Section 9204 permits a public entity to record a Notice of Completion on or within fifteen (15) days after the date of completion; and

WHEREAS, a timely recorded Notice of Completion shortens the period for service of stop payment notices and affects related payment-bond claim deadlines, and therefore is an important risk-management and project-closeout tool; and

WHEREAS, Civil Code Section 9204 requires a Notice of Completion to be signed and verified by the public entity or its agent and to contain the information required by applicable law; and

WHEREAS, District legal counsel has advised that District staff may accept completed work and execute and record Notices of Completion when the Board of Directors has expressly delegated that authority, subject to applicable law and District requirements; and

WHEREAS, the Board of Directors desires to establish an efficient, consistent, and controlled administrative process for acceptance of completed District public works and execution and recordation of Notices of Completion while preserving matters reserved to the Board.

NOW, THEREFORE, the Board of Directors of the West Valley Water District hereby resolves as follows:

SECTION 1. The General Manager, or the General Manager's written designee, is authorized to act under this Resolution only with respect to District-awarded public works projects and construction contracts for which the contract award and funding have been authorized in accordance with District policy and for which acceptance is not otherwise reserved to the Board of Directors.

SECTION 2. Before accepting a project, the General Manager or written designee shall receive a written or verbal recommendation from the responsible department head, supported by project closeout documentation, that the work is complete and eligible for acceptance under the contract documents and applicable law.

SECTION 3. Upon acceptance, the General Manager or written designee is authorized to execute and verify, and to cause it to be recorded, a Notice of Completion within the time permitted by applicable law, together with any ministerial recorder documents directly necessary for recordation. Each Notice

of Completion shall be in a form approved by District legal counsel and shall comply with applicable California Civil Code requirements.

SECTION 4. The General Manager or written designee may consult District legal counsel before accepting a project or recording a Notice of Completion if there is a material unresolved claim or dispute, known defective work, a surety issue, or another circumstance that may materially affect the District's rights or obligations. The General Manager or written designee is authorized to take all actions reasonably necessary to implement this Resolution.

SECTION 5. Nothing in this Resolution delegates authority to award contracts, approve project budgets, approve change orders or contract amendments beyond existing delegated authority, accept developer-installed facilities or other projects for which Board acceptance is required by law, contract, grant or financing terms, prior Board action, or District policy, or exercise any authority otherwise reserved to the Board of Directors.

SECTION 6. The General Manager shall report to the Board of Directors regarding actions taken under this Resolution. The report may identify each project and contractor, the date of acceptance, the Notice of Completion recordation date and recorder's document number, the approved contract amount as of acceptance, and any material outstanding claim or dispute.

SECTION 7. This Resolution shall take effect immediately upon adoption.

PASSED, APPROVED, and ADOPTED this ____ day of _____, 2026.

BOARD OF DIRECTORS

KELVIN MOORE, President
Board of Directors
West Valley Water District

ATTEST:

BRADON YOSHIDA, Board Secretary
West Valley Water District

CERTIFICATION

I, Brandon Yoshida Board Secretary of the West Valley Water District, do hereby certify that the foregoing Resolution No. 2026-11 was duly adopted by the Board of Directors of the West Valley Water District at a regular meeting held on _____, by the following vote:

AYES:	BOARD MEMBERS:
NOES:	BOARD MEMBERS:
ABSENT:	BOARD MEMBERS:
ASBSTAIN:	BOARD MEMBERS:

Dated: _____

BRANDON YOSHIDA, Board Secretary
West Valley Water District



STAFF REPORT

DATE: September 1, 2026

TO: Engineering, Operations and Planning Committee

FROM: Rocky Welborn, Director of Engineering

SUBJECT: Award a Construction Contract with Dominguez General Engineering, Inc. and Approve Task Order with Albert A. Webb Associates for the Bloomington Alleyway Main Replacement Phase 3B Project (W25036)

STRATEGIC GOAL:

Strategic Goal 1 - Manage and Deliver a Safe, Reliable, and Sustainable Water Supply; A. Increase System Capacity for Anticipated Growth

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

MEETING HISTORY:

None.

BACKGROUND:

The West Valley Water District (District) water distribution system service within the unincorporated County of San Bernardino, in the Bloomington area, consists of mains, service lines, meters, and valves located in the alleyways at the rear of the properties. To resolve access limitations and improve overall system reliability, the District proposed a project that included a new 8-inch (8") water distribution pipeline, approximately 5,800 linear feet, within the public right-of-way connecting to existing distribution mains at Locust and Cedar Avenues along 7th and 9th Streets, including reconnecting services with new piping from the main to the front of the properties within the area.

The Board of Directors authorized the professional services agreement (PSA) with Albert A. Webb Associates (Webb) for the design of the Zone 2 Waterline and Service Relocations in the Bloomington Area, Phase 3B Project (Project). Previous Task Orders consisted of the design and as-needed inspection services. Webb is knowledgeable about the project area and has successfully worked on the previous phases during construction activities, providing the necessary construction management and inspection services.

The 3B Project was awarded funding through the Environmental Protection Agency's Community Grants program with the support of Congresswoman Norma Torres in the amount of two million dollars (\$2,000,000.00). Staff has been trained to process reports and reimbursement requests with the EPA.

The project was determined to be categorically exempt under the California Environmental Quality Act (CEQA) in 2017. This item is in support of the District's Strategic Plan Goal to manage and deliver a safe, reliable, and sustainable water supply and strategy to apply planning efforts with best practices.

DISCUSSION:

Staff issued a Request for Bids (“RFB”) with a bid package that included Federal funding requirements such as the Davis-Bacon Act, American Iron and Steel (AIS), and Buy American Build America (BABA) provisions. This RFB was posted on PlanetBids and advertised in the local newspaper, The Sun, on June 13, 2026, and June 20, 2026, to comply with legal noticing requirements. The bidding process included a mandatory job walk which twenty (20) contractors attended. Staff received nine (9) responsive bids, and two (2) were deemed non-responsive. A breakdown of the bids received is provided in the table below:

<u>Bidder</u>	<u>Bid Amount</u>
Dominguez General Engineering, Inc.	\$4,427,861.00
Downing Construction, Inc.	\$5,110,182.00
Big Ben Engineering	\$5,589,582.00
TK Construction	\$5,702,346.00
T.E. Roberts, Inc.	\$5,724,988.00
C.P. Construction Co., Inc.	\$5,843,347.00
TBU Inc	\$5,916,749.65
Norstar Plumbing & Engineering, Inc.	\$5,967,425.60
J. A. Salazar Construction & Supply Corp.	\$7,502,319.60
EL-CO Contractors, Inc.	n/a
CEM Construction Corp.	n/a
Engineers Estimate	\$4,670,700.00

The basis of award instructed bidders to propose on base bid items for the minimum required work plus an additive bid item to grind and overlay the asphalt paving cap per the County of San Bernardino Department of Public Works requirements. Staff recommends including the additive bid item in the award as a flexibility to expand the project scope should the County require additional paving repairs beyond typical trench restoration.

The lowest, responsible, and responsive bid was submitted by Dominguez General Engineering, Inc., Pomona, CA. Staff subsequently reviewed the contractor’s licensing, bonding, references, and list of subcontractors submitted for the project and found that the bid proposal documentation met project requirements. Dominguez General Engineering, Inc.’s proposal is attached as **Exhibit A**, for a total amount of \$4,427,861.00.

Staff also requested the design engineer (Albert A. Webb Associates) provide a proposal to perform engineering services during construction and provide as-needed inspection services for the 3B Project. These services will include traditional project management responsibilities of the Engineer of Record, such as responding to requests for information from the Contractor and providing design intent responses, construction staking, and inspection that will support the District by augmenting staff. A new task order is necessary to retain Webb services for the duration of the construction phase. Webb has included these services in their proposal, attached as **Exhibit B**, for a total amount of \$161,100.00.

The estimated project construction costs are itemized below:

Project Task	Vendor	Totals
Construction	Dominguez General Engineering, Inc.	\$4,427,861.00
10% Construction Contingency Allowance ⁽¹⁾	As allowable per the Public Contract Code	\$44,278.61
Engineering Services During Construction & Inspection	Albert A. Webb Associates	\$161,100.00
Environmental Engineering Services	Tom Dodson & Associates (already approved)	\$14,780.00
TOTAL CONSTRUCTION COST		\$4,648,019.61

Note: (1) Note that public works contracts provide the General Manager authority to issue change orders. When the Board approves the contract, it approves this authority. Ten percent of the original project cost is the allowable aggregate under the Public Contract Code for changed conditions on a public works construction project, and by providing change order allowance authority upfront, the Board helps reduce the possibility of delay.

The expected construction duration for the proposal is 240 working days.

FISCAL IMPACT:

The project is included in the five-year funding schedule for the Capital Improvement Plan (CIP) Budget under Project No. W25036. Sufficient funds in Project No. W25036 have been allocated within the project budget to cover the anticipated total construction cost.

REQUESTED ACTION:

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

1. Approve a Construction Contract with Dominguez General Engineering, Inc. in the amount of \$4,427,861.00 for the construction services for W25036 - Bloomington Alleyway Main Replacement Phase 3B Project, and authorization to approve up to \$44,278.61 for 10% construction contract contingencies as allowable per the Public Contract Code for a Total Contract Value of \$4,472,139.61;
2. Approve a New Task Order with Albert A. Webb Associates in the amount of \$161,100 for engineering support and as-needed inspection services during construction for CIP Project No. W25036; and
3. Authorize the General Manager to execute all necessary documents.

Attachments

[Exhibit A - Public Works Agreement \(W25036\)](#) (Appendices Available for Review Upon Request)

[Exhibit B - Task Order No.6 - Albert A. Webb](#)

EXHIBIT A

WEST VALLEY WATER DISTRICT

AGREEMENT

ZONE 2 WATERLINE AND SERVICE RELOCATION IN THE BLOOMINGTON AREA, 7TH STREET, 9TH STREET, LINDEN AVENUE AND CEDAR AVENUE PHASE IIIB (W25036) EPA GRANT NO. 97T26401-0 PROJECT

This Contract is made this **17th** day of **September, 2026** between the West Valley Water District ("WVWD") and **Dominquez General Engineering, Inc.** ("Contractor"). WVWD and Contractor may be collectively referred to as "Parties" and individually as a "Party."

RECITALS

- A. WVWD is a public agency organized under the laws of the State of California, with power to contract for services necessary to achieve its purpose.
- B. WVWD desires to engage Contractor for performance of the following public work of improvement of the **Zone 2 Waterline And Service Relocation In The Bloomington Area, 7th Street, 9th Street, Linden Avenue and Cedar Avenue Phase IIIB (W25036)** Project (the "Project or the Work").
- C. Contractor represents that it is a licensed contractor pursuant to Section 7000 et seq. of the Business and Professions Code in the classification 724233 which it shall maintain for the duration of the Contract.
- D. Contractor further represents that it has examined and is fully familiar with all of the provisions of the Contract Documents; that it has satisfied itself as to the nature and location of all Work, the general and local conditions to be encountered in the performance of any Work, and all other matters which can in any way affect the Work or the cost thereof.
- E. Contractor has submitted a proposal to WVWD, incorporated herein by this reference, to perform all work and furnish the labor, supervision, materials and equipment, and operations necessary and required to complete the Project in strict accordance with the provisions of the Contract Documents, and at the prices stated.
- F. The Parties desire to enter into this Agreement for the purpose of setting forth the terms and conditions upon which the Contractor shall complete the Project.

SECTION 1 - SCOPE

- A. Contractor shall furnish all necessary management, supervision, labor, materials, tools, supplies, equipment, plant, services, engineering, testing and/or any other act or thing required to diligently and fully perform and complete the Project in accordance with the Contract Documents, which is generally described as follows:

SUMMARY OF SCOPE.

Without limiting the foregoing description, Contractor's scope of work includes, but is not limited to, the following:

- 1. Submit any required samples, product data, certificates, operations and maintenance instructions, guarantees, and other submittals no later than 60 working days after the date WVWD issues a Notice to Proceed and before the preconstruction meeting.
- 2. Submit a list of any permits and licenses the Contractor shall obtain indicating the

agency granting the permit, the expected date to submit the application, and the required date for the receipt of the permit.

3. Protect all materials to be used in the Work in accordance with the specifications.
 4. Protect existing facilities and personal property.
 5. Attend a preconstruction conference with WVWD to discuss schedule, access, sequence of work, and other issues.
 6. If requested by WVWD, prepare and submit a written daily activity report to WVWD for each day on which work is performed, including weekends and holidays when worked, and submit reports to WVWD no later than the next business day. The daily reports shall, at a minimum, include the following information: construction activities and locations, construction crew sizes of general and subcontractors, start or completion of activities, progress on construction activities (including units or portions of work completed), tests or inspections performed, deliveries of material or equipment, delays or potential delays, visitors to the site, weather conditions, construction equipment used, and personal injuries or damage to property.
 7. The Contractor shall be responsible for unloading, hoisting and otherwise handling its own materials, supplies and equipment.
 8. Coordinate with owner-scheduled events.
 9. The Contractor is responsible for researching and complying with all local codes, agencies and jurisdictions that regulate and govern the Work.
 10. Contractor shall set up, identify, coordinate, provide safe access, and obtain all inspections for its work, as required by any authorized agency or applicable code, prior to covering up work.
- B. The following documents are incorporated into and made part of this Contract by this reference:
1. Insurance (Attachment A)
 2. Designation of Subcontractors (Attachment B)
 3. Public Works Contractor Registration Certification (Attachment C)
 4. Contractor's Proposal (Attachment D)
 5. Payment and Performance Bonds (Attachment E)
 6. Change orders issued in accordance with the Contract Documents
- C. These documents shall be referred to collectively as the "Contract Documents." The Contract Documents are intended to be complementary, and a requirement in one document is as effective as if it appeared in all of the Contract Documents. In the event of a conflict between any of the Contract Documents, the documents shall be given effect in the following order: Change Orders (most recent first), Addenda (most recent first), Contract, Insurance Requirements, and Contractor's Proposal/Schedule of Pay Items.
- D. Contractor shall comply with all requirements of the Contract Documents. Where there is a conflict between the requirements of the Contract Documents, the more stringent requirements shall govern.

SECTION 2 - PRICE

- A. WVWD agrees to pay, and Contractor agrees to accept, the sum of **Four Million, Four**

Hundred Twenty-Seven Thousand, Eight Hundred Sixty-One Dollars And Zero Cents (\$4,427,861.00) (the "Contract Price") subject to adjustments for changes in the work as may be directed in writing by WVWD, as payment in full for the Work. Work to be done at unit prices will be paid based on actual quantities of work performed and accepted.

- B. Contractor shall submit a payment application for the total work completed once each month and upon completion of the Project and satisfaction of all conditions of the Contract Documents. WVWD shall make payment within thirty (30) days of receipt of an undisputed payment application, less five percent retention. WVWD shall release the retained funds (less any amounts in dispute, deducted for liquidated damages or as required by law, or other offsets) no less than thirty-five (35) days after the date WVWD accepts the Work. Pursuant to Public Contract Code section 22300, for monies earned by the Contractor and withheld by WVWD to ensure the performance of the Contract, the Contractor may, at its option, choose to substitute securities meeting the requirements of Public Contract Code section 22300.

If any of the Work is to be paid based on unit prices, Contractor shall submit a monthly itemized estimate of Work done for the purpose of making progress payments. Contractor shall submit, with each of its payment requests, an adjusted list of actual quantities, verified by WVWD, for unit price items listed, if any, in the Schedule of Pay Items. Following WVWD's acceptance of the Work, the Contractor shall submit to WVWD a written statement of the final quantities of unit price items for inclusion in the final payment request. WVWD shall have the right to adjust any estimate of quantity and to subsequently correct any error made in any estimate for payment. WVWD makes no representation that the actual quantities of work performed will not vary from the estimates

- C. Contractor agrees to furnish, as a condition of payment, payroll affidavits, receipts, vouchers, certified payroll reports, and other documents, in form satisfactory to WVWD, prior to receipt of any payment. Contractor shall submit Conditional and Unconditional waivers and release of lien upon (as provided in Civil Code sections 8132, 8134, 8136, and 8138) on behalf of itself, subcontractors and suppliers that furnished labor, material, equipment or services to the Project.
- D. In accordance with California Public Contract Code Section 22300, WVWD will permit the substitution of securities for any monies withheld by WVWD to ensure performance under the Contract. At the request and expense of the Contractor, securities equivalent to the amount withheld shall be deposited with WVWD, or with a state or federally chartered bank in California as the escrow agent, and thereafter WVWD shall then pay such monies to the Contractor as they come due. Upon satisfactory completion of the Contract, the securities shall be returned to the Contractor. For purposes of this Section and Section 22300 of the Public Contract Code, the term "satisfactory completion of the contract" shall mean the time WVWD has issued written final acceptance of the Work and filed a Notice of Completion as required by law and provisions of this Contract. The escrow agreement used for the purposes of this Section shall be in the form provided by WVWD.

SECTION 3 - ENTIRE AGREEMENT

This Contract represents the entire agreement between WVWD and Contractor and supersedes any prior written or oral representations. No oral order, objection, direction, claim or notice by any party or person shall affect or modify any of the terms or obligations contained in the Contract Documents.

SECTION 4 - TIME

- A. Contractor shall complete the Project no later than **Two Hundred Forty (240) Working**

Days following WVWD's issuance of the Notice to Proceed (the "Contract Time").

- B. Contractor shall provide WVWD with scheduling information in a form acceptable to WVWD, including any changes made by WVWD in the scheduling of work. Contractor shall coordinate its work with that of all other contractors, subcontractors and suppliers so as not to delay or damage their performance.
- C. If Contractor fails to complete the Project within the Contract Time, WVWD will sustain damage. It is and will be impracticable to determine the actual damage which WVWD will sustain in the event of and by reason of such delay; therefore, Contractor will pay to WVWD the sum of **\$1,000.00** for each and every calendar day beyond expiration of the Contract Time. Contractor agrees to pay such liquidated damages as herein provided, and in case the same are not paid, agrees that WVWD may deduct the amount thereof from any monies due or that may become due to the Contractor under the Contract.
- D. It is further agreed that in case Contractor fails to complete the Project in all parts and requirements within the Contract Time, WVWD shall have the right to extend the Contract Time or not, as may seem best to serve the interest of WVWD; and if it decides to extend Contract Time, WVWD shall further have the right to charge to the Contractor, his heirs, assigns or sureties, and to deduct from the final payment for the work, all or any part, as it may deem proper, of the actual cost of engineering, inspection, superintendence, and other overhead expenses directly chargeable to the Contract that accrue during the period of such extension.
- E. The Contractor will not be assessed with liquidated damages or the cost of engineering and inspection during the delay in the completion of the Project caused solely by acts of God or of the public enemy, fire, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather or delays of subcontractors due to such causes, provided that the Contractor shall within three (3) days from the beginning of any such delay, notify WVWD, in writing of the causes of delay. WVWD shall ascertain the facts and the extent of delay, and his findings thereon shall be final and conclusive.
- F. As an express condition of any adjustment of the Contract Time or Contract Price on account of delay, including delay caused by acts of WVWD, Contractor must give WVWD written notice of the commencement of delay within three (3) days of its occurrence.

SECTION 5 - LABOR

- A. **Prevailing Wages.** The Contract is subject to California Labor Code Sections 1720 et seq., and Contractor and any subcontractor shall pay not less than the specified prevailing rates of wage to all workers employed in performance of the Work. Pursuant to the provisions of Section 1770 of the California Labor Code, WVWD has obtained the general prevailing rate of wages and employer payments for health and welfare, vacation, pension and similar purposes, as determined by the Director of the Department of Industrial Relations, a copy of which is on file in the office of WVWD, and shall be made available for viewing to any interested party upon request. The Contractor and each subcontractor shall forfeit as a penalty to WVWD not more than Two Hundred Dollars (\$200) for each calendar day, or portion thereof, for each worker paid less than the stipulated prevailing wage rate in violation of the Labor Code. In addition, the difference between the prevailing wage rate and the amount paid to each worker for each calendar day or portion thereof for which each worker was paid less than the stipulated prevailing wage rate shall be paid to each worker by the Contractor.
- B. **Employment of Apprentices.** Contractor's attention is directed to the provisions in Section 1777.5 and 1777.6 of the Labor Code concerning the employment of apprentices by the

Contractor or any subcontractor under the Contractor. It shall be the responsibility of the Contractor to effectuate compliance on the part of itself and any subcontractors with the requirements for employment of apprentices. Information relative to apprenticeship standards, wage schedules, and other requirements may be obtained from the Director of Industrial Relations, ex-officio the Administrator of Apprenticeship, San Francisco, California, or from the Division of Apprenticeship Standards and its branch offices.

- C. Payroll Records. Pursuant to Labor Code Section 1776, the Contractor and each subcontractor shall maintain weekly certified payroll records showing the name, address, social security number, work classification, straight time and overtime hours paid each day and week, and the actual per diem wages paid to each journeyman, apprentice, worker or other employee employed in connection with the work. Contractor shall certify under penalty of perjury that records maintained and submitted by Contractor are true and accurate. Contractor shall also require subcontractor(s) to certify weekly payroll records under penalty of perjury. In the event of noncompliance with the requirements of this Section, the Contractor shall have ten (10) days in which to comply subsequent to receipt of written notice specifying any item or actions necessary to achieve compliance with this section. If Contractor or subcontractor does not comply after such ten (10)-day period, the Contractor shall, as a penalty to WVWD, forfeit One Hundred Dollars (\$100) for each day, or portion thereof, for each worker until strict compliance is effectuated.

In accordance with Labor Code section 1771.4, the Contractor and each subcontractor shall furnish the certified payroll records directly to the Department of Industrial Relations on a weekly basis and in the format prescribed by the Department of Industrial Relations, which may include electronic submission. Contractor shall comply with all requirements and regulations from the Department of Industrial Relations relating to labor compliance monitoring and enforcement.

- D. Public Works Contractor Registration

Pursuant to Labor Code sections 1725.5 and 1771.1, all contractors and subcontractors that wish to bid on, be listed in a bid proposal, or enter into a contract to perform public work must be registered with the Department of Industrial Relations. No bid will be accepted nor any contract entered into without proof of the contractor's and subcontractors' current registration with the Department of Industrial Relations to perform public work. Contractor and its subcontractors, of any tier, shall maintain active registration with the Department of Industrial Relations for the duration of the Project. To this end, Contractor shall execute the Public Works Contractor Registration Certification attached hereto as Attachment C, attesting to the facts contained therein. In addition, Contractor shall provide the registration number for each listed subcontractor in the space provided in the Designation of Subcontractors Form attached hereto as Attachment B.

This Project is subject to compliance monitoring and enforcement by the Department of Industrial Relations. In executing this contract, Contractor acknowledges that it has reviewed all applicable labor compliance requirements and included the cost of complying with such requirements in its bid.

- E. Hours of Work.

1. Eight (8) hours of work shall constitute a legal day's work. The Contractor and each subcontractor shall forfeit, as penalty to WVWD, twenty-five dollars (\$25) for each worker employed in the execution of Work by the Contractor or any subcontractor for each day during which such worker is required or permitted to work more than eight (8) hours in any one day and forty (40) hours in any week in violation of the provisions of the California Labor Code, and in particular, section 1810 to section 1815, except as provided in Labor Code section 1815.

2. The Contractor shall perform all work during the hours of 7:00 a.m. to 3:30 p.m., Monday through Friday unless otherwise authorized by WVWD in writing. If the Contractor wishes to work during any other hours or on weekends, written permission must be received from WVWD. The request must be received at least two (2) working days in advance of any work. No work will be allowed on WVWD Holidays except in the case of an emergency. A listing of WVWD holidays is on file in the office of WVWD. If Contractor requests overtime work in which WVWD will incur costs, Contractor shall be responsible for payment of WVWD's costs incurred in connection with the overtime work. WVWD will invoice the Contractor at time and one half to cover the costs incurred. If Contractor does not pay the invoice within ten (10) days, WVWD may deduct the amount billed from other payments due or to become due to Contractor under the Contract.
 3. Pursuant to Federal Regulations under 40 U.S.C. 3702 of the Contract Work Hours and Safety Standards Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.
- F. Labor Compliance. Contractor shall post, at appropriate conspicuous points on the Project site, a schedule showing all determined general prevailing wage rates and all authorized deductions, if any, from unpaid wages actually earned.
- G. Labor Certification. Pursuant to the requirements of Division 4 of the Labor Code, the Contractor will be required to secure the payment of worker's compensation to its employees in accordance with the provisions of section 3700 of the Labor Code. Prior to commencement of work, the Contractor shall sign and file with the Engineer a certification in the following form:
- "I am aware of the provisions of section 3700 of the Labor Code which require every employer to be insured against liability for worker's compensation or to undertake self- insurance in accordance with the provisions before commencing the performance of the work of this contract."
- H. Full compensation for conforming to the requirements of this section shall be considered as included in the Contract Price, and no additional compensation will be allowed therefore.

SECTION 6 - CHANGES IN WORK

- A. Contractor shall make no changes in the Work without written direction from WVWD. Contractor shall not be compensated for any change made without WVWD's written direction. No changes in the work covered by this Contract shall exonerate any surety or any bond given in connection with this Agreement.
- B. If WVWD directs the Contractor in writing to make changes in the work that materially affect the cost of performing the work, the Contract Price will be adjusted based on one of the following:
 1. Where the work involved is covered by unit prices contained in the Contract Documents, by application of unit prices to the quantities involved in the changed

Work;

2. By a combination of existing and new unit prices and related quantities for the changed work;
 3. Time and Materials, calculated as set forth in Section 6(C), below; or
 4. By mutual acceptance of a lump sum.
- C. The cost for extra or changed work performed on a Time and Materials basis shall be determined as follows:
1. Labor: Contractor will be paid cost of labor for workers used in actual and direct performance of extra work, including only actual wages paid shall include any employer payments to or on behalf of workers for health and welfare, pension, vacation, and similar purposes.
 2. Material: Only materials furnished by Contractor and necessarily used in performance of extra Work will be paid for. Cost of such materials will be cost, including sales tax and delivery charges, to purchaser (Contractor, Subcontractor or other forces) from supplier thereof.
 3. Equipment: For Contractor-owned equipment, payment will be made at rental rates listed for equipment in the California Department of Transportation official equipment rental rate schedule which is in effect on the date upon which extra Work is accomplished and which schedule is incorporated herein by reference as though fully set forth herein. If there is no applicable rate for an item of equipment, then payment shall be made for Contractor-owned equipment at rental rate listed in the most recent edition of the Association of Equipment Distributors (AED) book.
 - (a) For rented equipment, payment will be made based on actual rental invoices. Equipment used on extra Work shall be of proper size and type.
 - (b) Rental rates paid shall be deemed to cover cost of fuel, oil, lubrication, supplies, small tools, necessary attachments, repairs and maintenance of any kind, depreciation, storage, insurance, and all incidentals. Unless otherwise specified, manufacturer's ratings, and manufacturer-approved modifications, shall be used to classify equipment for determination of applicable rental rates. Rental time will not be allowed while equipment is inoperative due to breakdowns.
 - (c) Individual pieces of equipment or tools having a replacement value of \$100 or less, whether or not consumed by use, shall be considered to be small tools.
 4. Work Performed by Special Forces or Other Special Services: When WVWD and Contractor, by agreement, determine that special service or item of extra Work cannot be performed by forces of Contractor or those of any Subcontractors, service or extra Work item may be performed by specialist. Invoices for service or item of extra Work on basis of current market price thereof may be accepted without complete itemization of labor, material, and equipment rental costs when it is impracticable and not in accordance with established practice of special service industry to provide complete itemization. In those instances, wherein Contractor is required to perform extra Work necessitating a fabrication or machining process in a fabrication or machine shop facility away from Site, charges for that portion of extra Work performed in such facility may, by agreement, be accepted as a specialist billing. In lieu of overhead and profit provided in paragraph 5(a), below, fifteen percent (15%) will be added to specialist invoice price, after deduction of any cash or trade discount offered or available, whether or not such discount may have been taken.

5. Overhead Defined. The following constitutes charges that are deemed included in overhead for all Contract Modifications, including work performed on a Time and Materials basis. Contractor shall not invoice or receive payment for these costs separately: Drawings: field drawings, Shop Drawings, etc., including submissions of drawings; Routine field inspection; General Superintendence; General administration and preparation of cost proposals, schedule analysis, Change Orders, and other supporting documentation; Computer services; Reproduction services; Salaries of project engineer, superintendent, timekeeper, storekeeper, and secretaries; Janitorial services; Small tools, incidentals and consumables; Temporary on-Site facilities (Offices, Telephones, Plumbing, Electrical Power, Lighting; Platforms, Fencing, Water, Home office expenses; vehicles and fuel used for work otherwise included in the Contract Documents; Surveying; Estimating; Protection of Work; Handling and disposal fees; Final cleanup; Other incidental Work; Related warranties.
 6. Overhead and Profit for Time and Materials. For work Contractor performs on Time and Materials at WVWD's direction, the following markups will be added to the cost of labor, materials and equipment, calculated as described above.
 - (a) Overhead and profit on labor shall be fifteen percent (15%).
 - (b) Overhead and profit on materials shall be fifteen percent (15%).
 - (c) Overhead and profit on equipment rental shall be ten percent (10%).
 - (d) On proposals covering both increases and decreases in Contract Price, overhead and profit shall be allowed on the net increase only as determined in this paragraph. When the net difference is a deletion, no percentage for overhead or profit will be allowed, but rather a deduction shall apply.
 - (e) The markup shall include profit, small tools, cleanup, supervision, warranties, cost of preparing the cost proposal, jobsite overhead, and home office overhead. No markup will be allowed on taxes, insurance, and bonds.
- D. If WVWD directs the Contractor in writing to make changes in the Work that materially affect the time required to perform the Work, WVWD will make a reasonable adjustment to the Contract Time.

SECTION 7 - CLAIMS AND DISPUTES

- A. If any dispute shall arise between WVWD and Contractor regarding performance of the work, or any alleged change in the work, Contractor shall timely perform the disputed work and shall give written notice of a claim for additional compensation for the work to WVWD within three (3) days after commencement of the disputed work. Contractor's failure to give written notice within the three (3)-day period constitutes an agreement by Contractor that it will receive no extra compensation for the disputed work.
- B. If a claim cannot be resolved through direct discussions between WVWD and Contractor, disputes for \$375,000 or less shall be handled in accordance with Public Contract Code Sections 20104 et seq. WVWD shall respond in writing within the statutory time period(s), or, may request in writing within 30 Days of receipt of the claim, any additional documents supporting the claim or relating to defenses or claims WVWD may have against the claimant. If additional information is needed thereafter, it shall be provided upon request. WVWD's response shall be submitted within the statutory timeframe after receipt of the further documents, or within the same period of time taken by the claimant to produce the additional information or documents, whichever is greater. The Contractor shall make these records and documents available at all reasonable times, without any direct charge.

- C. If a claim is more than \$375,000, WVWD shall respond in writing within a reasonable period of time to review and analyze the claim. The parties also agree to participate in mediation with a mutually agreeable mediator following an exchange of documents reasonably necessary for resolution of the issues in dispute.
- D. If the claimant disputes WVWD's response, or if WVWD fails to respond within the statutory time period(s), the claimant may so notify WVWD within 15 Days of the receipt of the response or the failure to respond, and demand an informal conference to meet and confer for settlement. Upon such demand, WVWD shall schedule a meet and confer conference within 30 Days.
- E. If following the meet and confer conference, the claim or any portion thereof remains in dispute, the claimant may file a claim pursuant to Government Code sections 900 et seq. and Government Code sections 910 et seq. For purposes of those provisions, the time within which a claim must be filed shall be tolled from the time the claimant submits the written claim until the time the claim is denied, including any time utilized for the meet and confer conference.
- F. Submission of a claim, properly certified, with all required supporting documentation, and written rejection or denial of all or part of the claim by WVWD, is a condition precedent to any action, proceeding, litigation, suit, or demand for arbitration by Contractor.
- G. Venue for any litigation arising out of or relating to this Contract shall be Riverside County, California.
- H. Pursuant to Public Contract Code section 9201, WVWD shall provide Contractor with timely notification of the receipt of any third-party claim relating to the Contract.

SECTION 8 - INSPECTION AND PROTECTION OF WORK

- A. Responsibility for, and security of, all work and materials is the responsibility of the Contractor until final acceptance of the Project by WVWD.
- B. All Work shall be inspected by WVWD. The charges for inspection shall be in accordance with WVWD's regulations. If WVWD is unable to provide an inspector or inspectors, Contractor shall reschedule the Work for another time at no cost to WVWD. Work performed without inspection shall be rejected.
- C. Contractor shall make the work accessible at all reasonable times for inspection by WVWD. Contractor shall, at the first opportunity, inspect all material and equipment delivered to the jobsite by others to be used or incorporated in the Contractor's work and give prompt notice of any defect therein. Contractor assumes full responsibility to protect the work done hereunder until final acceptance by WVWD.
- D. When the Work is completed, Contractor shall request, in writing, a final inspection. Within ten (10) days of the receipt of such request, WVWD shall make a final inspection. The Contractor or its representatives may be present at the final inspection. The purpose of such final inspection shall be to determine whether the Work has been completed in accordance with the Contract Documents, including all change orders and all interpretations and instructions previously issued.
- E. WVWD may reject materials or Work that does not meet the requirements of the Contract Documents. If WVWD does so, Contractor shall promptly remove the rejected materials or work and replace it with materials or work that meet the requirements of the Contract Documents, at no additional cost to WVWD.

SECTION 9 - ASSIGNMENT AND SUBCONTRACTING

- A. Contractor shall give personal attention to the performance of the Contract and shall keep the Work under its control.
- B. No subcontractors will be recognized as such, and all persons engaged in the work of construction will be considered as employees of the Contractor, who will be held responsible for their work which shall be subject to the provisions of the Contract and specifications.
- C. No subcontractor who is ineligible to bid work on, or be awarded, a public works project under Labor Code sections 1771.1 or 1777.7 can bid on, be awarded or perform work as a subcontractor on the Project. The Contractor is prohibited from performing work on the Project with a subcontractor who is ineligible to perform work on a public works project under these sections of the Labor Code.
- D. When a portion of the work which has been subcontracted by the Contractor is not being prosecuted in a manner satisfactory to WVWD, the subcontractor shall be removed immediately on the request of WVWD in the manner required by law and shall not again be employed on the work.
- E. Contractor shall not assign any portion of the work to be performed under this Agreement or any of the rights or obligations under this Agreement, without the prior written consent of WVWD, which consent may be withheld in WVWD's sole and absolute discretion.

SECTION 10 - TERMINATION

- A. Should Contractor fail within seven (7) calendar days from receipt of WVWD's written notice to correct any default, including but not limited to failure to perform the Work in accordance with the Contract Documents, failure to comply with the directions of WVWD, or failure to pay its creditors, WVWD may terminate this Contract and/or, in its sole discretion, make a demand on Contractor's performance bond surety. Following a termination for default, WVWD shall have the right to take whatever steps it deems necessary to complete the Project and correct Contractor's deficiencies and charge the cost thereof to Contractor, who shall be liable for the full cost of WVWD's corrective action, including reasonable overhead, profit and attorneys' fees.
- B. WVWD also reserves the right at any time to terminate the Contract at WVWD's convenience upon five (5) days written notice to Contractor if WVWD believes, in its sole discretion, that it is in the best interest of the WVWD to do so. In the event of termination for convenience, Contractor shall recover only the actual cost of work completed to the date of termination, which costs are documented to WVWD's satisfaction, calculated in accordance with Section 6, above. Contractor shall not be entitled to any claim or lien against WVWD for any additional compensation or damages in the event of such termination. Any award under this procurement process is not exclusive and the WVWD reserves the right to purchase goods and services from other contractors when it is in the best interest of the WVWD.
- C. Pursuant to Federal Regulations, when federal funds are expended by the West Valley Water District, the West Valley Water District reserves the right to immediately terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Contractor, in the event contractor fails to: (1) meet schedules, deadlines, and/or delivery dates within the time specified in the procurement solicitation, contract, and/or a purchase order; (2) make any payments owed; or (3) otherwise perform in accordance with the contract and/or the procurement solicitation.
- D. If WVWD terminates Contractor for cause, and if it is later determined that the termination was wrongful, such default termination shall automatically be converted to and treated as a

termination for convenience. In such event, Contractor shall be entitled to receive only the amounts payable under this section, and Contractor specifically waives any claim for any other amounts or damages, including, but not limited to, any claim for consequential damages or lost profits.

SECTION 11 - HOLD HARMLESS AND INDEMNIFICATION

- A. WVWD and all officers and employees thereof connected with the Work, shall not be answerable or accountable in any manner: for any loss or damage that may happen to the Work or any part thereof; for any loss or damage to any of the materials or other things used or employed in performing the Work; for injury to or death of any person; or for damage to property from any cause except losses due to sole or active negligence of WVWD's officers or employees.
- B. Contractor shall indemnify, defend with legal counsel approved by WVWD, and hold harmless WVWD, its officers, officials, employees and volunteers from and against all liability, loss, damage, expense, cost (including without limitation reasonable legal counsel fees, expert fees and all other costs and fees of litigation) of every nature arising out of or related to the Work or the Project, except such loss or damage which is caused by the sole or active negligence or willful misconduct of WVWD. Should conflict of interest principles preclude a single attorney from representing both WVWD and Contractor, or should WVWD otherwise find Contractor's legal counsel unacceptable, then Contractor shall reimburse WVWD its costs of defense, including without limitation reasonable attorney's fees, expert fees and all other cost and fees of litigation. The Contractor shall promptly pay any final judgment rendered against WVWD (and its officers, officials, employees and volunteers) except for claims determined by a trier of fact to have been the result of WVWD's sole or active negligence or willful misconduct. The foregoing provisions are intended to be as broad and inclusive as is permitted by the law of the State of California and will survive termination of this Agreement.
- C. Contractor's obligations under this section apply regardless of whether or not such claim, charge, damage, demand, action, proceeding, loss, stop notice, cost, expense, judgment, civil fine or penalty, or liability was caused in part or contributed to by an indemnified party. However, without affecting the rights of WVWD under any provision of this agreement, Contractor shall not be required to indemnify and hold harmless WVWD for liability attributable to the active negligence of WVWD, provided such active negligence is determined by agreement between the parties or by the findings of a court of competent jurisdiction. In instances where WVWD is shown to have been actively negligent and where WVWD's active negligence accounts for only a percentage of the liability involved, the obligation of Contractor will be for that entire portion or percentage of liability not attributable to the active negligence of WVWD.
- D. In addition to any remedy authorized by law, contract funds sufficient to pay for any claim may be retained by WVWD until disposition has been made of such suits or claims for damage.

SECTION 12 - BONDS AND INSURANCE

- A. Bonds.
 - 1. Within fifteen (15) working days after being notified of the award of the contract, and before WVWD will execute this Agreement, the Contractor shall furnish and file with WVWD Performance and Payment Surety bonds as set forth below.
 - 2. Contractor shall submit the bonds on the forms provided and include in Attachment

E, attached hereto, duly executed by a responsible corporate surety listed in the United States Department of the Treasury circular entitled "Companies Holding Certificates of Authority as Acceptable Sureties on Federal Bonds and as Acceptable Reinsuring Companies," authorized to do business in the State of California and acceptable to WVWD conditioned upon the faithful performance by the Contractor of all requirements of the Contract Documents. Each of the bonds shall be in a sum no less than one hundred percent (100%) of the Contract Price.

B. Insurance.

1. Contractor shall obtain, at its sole cost and expense, all insurance required and included in Attachment A. Certificates of such insurance and copies of the insurance policies and endorsements shall be delivered to WVWD within fifteen (15) working days after being notified of the award of the contract, and before execution of this Agreement by WVWD.

SECTION 13 - WARRANTY

Contractor warrants to WVWD that all materials and equipment furnished shall be new, free from faults and defects and of good quality and conform to the requirements of the Contract Documents.

Contractor hereby warrants its work against all deficiencies and defects for the period required by the Contract Documents or the longest period permitted by California law, whichever is greater. Unless otherwise stated in the Contract Documents, warranty periods shall begin upon the filing of the Notice of Completion and shall be for two years.

This Article shall not limit WVWD's rights under this Contract or with respect to latent defects, gross mistakes, or fraud. WVWD specifically reserves all rights related to defective work, including but not limited to defect claims pursuant to California Code of Civil Procedure section 337.15.

SECTION 14 - LAWS TO BE OBSERVED

- A. Contractor shall keep itself fully informed of all existing and future state and federal laws and county and municipal ordinances and regulations that in any manner affect those engaged or employed in the work, or the materials used in the work, or which in any way affect the conduct of work, and of all such orders and decrees of bodies or tribunals having any jurisdiction or authority over the same.
- B. Contractor shall at all times observe and comply with, and shall cause all of its agents and employees to observe and comply with all such existing and future Federal, State and local laws, ordinances, regulations, orders, and decrees of bodies or tribunals having any jurisdiction or authority over the Project; and shall protect and indemnify WVWD, and all officers and employees thereof connected with the Project, against any claim or liability arising from or based on the violation of any such law, ordinance, regulation, order, or decree, whether by WVWD's representative or their employees. If any discrepancy or inconsistency is discovered in the plans, drawings, specifications, or contract for the work in relation to any such law, ordinance, regulation, order or decree, Contractor shall promptly report the same to WVWD in writing.
- C. This Contract shall be governed by and construed in accordance with the laws of the State of California.
- D. Contractor shall agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251- 1387), as amended.

E.

SECTION 15 - CLEAN-UP

Contractor will remove from the project site all debris resulting from performance of the Work no less often than daily. If Contractor fails to do so, WVWD may, after twenty-four (24) hours' notice to Contractor, clean up the site and deduct the cost from the Contract Price.

SECTION 16 - STATE LICENSE BOARD NOTICE

Contractors are required by law to be licensed and regulated by the Contractors' State License Board which has jurisdiction to investigate complaints against contractors if a complaint regarding a patent act or omission is filed within four (4) years of the date of the alleged violation. A complaint regarding a latent act or omission pertaining to structural defects must be filed within ten (10) years of the date of the alleged violation. Any questions concerning a contractor may be referred to the Registrar, Contractors' State License Board, P.O. Box 26000, Sacramento, California 95826.

SECTION 17 - COMPLIANCE WITH STATE STORM WATER PERMIT

Contractor shall be required to comply with all aspects of the State Water Resources Control Board (State Water Board) Water Quality Order No. 2009-0009-DWQ, including any and all subsequent amendments and National Pollutant Discharge Elimination System General Permit for Storm Water Discharges Associated with Construction Activity (Permit) for all projects that involve construction on or disturbance of one acre or more of land or which are part of a larger common area of development.

SECTION 18 - MISCELLANEOUS

A. Existing Utilities.

The location of known existing utilities and pipelines are shown on the Plans in their approximate locations. However, nothing herein shall be deemed to require WVWD to indicate the presence of existing service laterals or appurtenances whenever the presence of such utilities on the site of the Project can be inferred from the presence of other visible facilities, such as buildings, cleanouts, meter and junction boxes, on or adjacent to the site of the Project. Underground facilities not known to WVWD may exist, or be in a location different from that which is shown in the Contract Documents.

Contractor shall take all steps reasonably necessary to ascertain the exact location of all underground facilities prior to doing work that may damage such facilities or interfere with their service, including but not limited to calling Underground Service Alert to locate utilities in accordance with the procedures described in Government Code section 4215 et seq. Contractor shall protect from damage any utility facilities that are to remain in place, be installed, relocated or otherwise rearranged. The Contractor shall not be entitled to additional compensation nor time extensions for work necessary to avoid interferences nor for repair to damaged utilities if the Contractor does not expose all such existing utilities as required by this section.

After the utility survey is complete, the Contractor shall commence "potholing" or hand digging to determine the actual location of the pipe, duct, or conduit. Contractor shall notify WVWD before starting potholing operations. The Contractor shall uncover all piping and conduits to a point one (1) foot below the pipe, where crossings, interferences, or connections are shown on the Drawings, prior to trenching or excavating for any pipe or structures, to determine actual elevations. New pipelines shall be laid to such grade as to clear all existing facilities which are to remain in service for any period subsequent to the construction of the run of pipe

involved.

The Contractor's attention is directed to the requirements of Government Code section 4216.2 (a)(2) which provides: "When the excavation is proposed within 10 feet of a high priority subsurface installation, the operator of the high priority subsurface installation shall notify the excavator of the existence of the high priority subsurface installation prior to the legal excavation start date and time, as such date and time are authorized pursuant to paragraph (1) of subdivision (a) of section 4216.2. The excavator and the operator or its representative shall conduct an onsite meeting at a mutually-agreed-upon time to determine actions or activities required to verify the location of the high priority subsurface installation prior to start time." The Contractor shall notify WVWD in advance of this meeting.

If the Contractor is required to locate, repair damage not due to the Contractor's failure to exercise reasonable care, and remove or relocate existing main or trunk line utility facilities, it shall be compensated under Section 6 of this Contract – Changes in the Work – including payment for equipment on the Project necessarily idled during such work.

The right is reserved by WVWD and the owners of underground facilities or their authorized agents, to enter the job for the purpose of making such changes as are necessary for the rearrangement of their facilities or for making necessary connection or repairs to their properties. The Contractor shall cooperate with forces engaged in such work and shall conduct its operations in such a manner as to avoid any delay or hindrance to the work being performed by such other forces.

B. Differing Site Conditions.

1. The Contractor shall promptly, and before the following conditions are disturbed, notify WVWD in writing of any:
 - (a) Material that the Contractor believes may be material that is hazardous waste, as defined in section 25117 of the Health and Safety Code, that is required to be removed to a Class I, Class II, or Class III disposal site in accordance with provisions of existing law,
 - (b) Subsurface or latent physical conditions at the site differing materially from those indicated by information about the site made available to bidders before the deadline for submitting bids, or
 - (c) Unknown physical conditions at the site of any unusual nature, differing materially from those ordinarily encountered and generally recognized as inherent in work of the character provided for in this Contract.
2. Contractor shall give Notice in accordance with the Change Order provisions above.
3. WVWD shall promptly investigate the conditions, and if it finds that such conditions do materially so differ, or do involve hazardous waste, and cause an increase or decrease in the Contractor's cost of, or the time required for, performance of any part of the Work, it shall issue a change order under the provisions described in the Contract Documents.
4. No claim of the Contractor under this clause shall be allowed unless the Contractor has given the notice required in the Contract Documents.
5. In the event a dispute arises between WVWD and the Contractor as to whether the conditions materially differ, or involve hazardous waste, or cause a decrease or increase in the Contractor's cost of, or time required for, performance of any part of the work, Contractor shall not be excused from completing the Work as provided in the Contract Documents. The Contractor shall proceed with all work to be performed

under the Contract. The Contractor shall retain any and all rights provided either by this Contract or by law, which pertain to the resolution of disputes and protests.

C. Records and Audits.

1. Contractor and its subcontractors shall establish and maintain records pertaining to this Contract. Contractor's and subcontractors' accounting systems shall conform to generally accepted accounting principles and all records shall provide a breakdown of all costs charged under this contract, including properly executed payrolls, time records, invoices and vouchers.
2. Contractor shall permit WVWD and its authorized representatives to inspect, examine and make copies of Contractor's books, records, accounts, and any and all data relevant to this Contract at any reasonable time for the purpose of auditing and verifying statements, invoices, or bills submitted by Contractor pursuant to this contract and shall provide such assistance as may be reasonably required in the course of such inspection. WVWD further reserves the right to examine and re-examine said books, records, accounts, and data during the four (4)-year period following the termination of this Contract; and Contractor shall in no event dispose of, destroy, alter, or mutilate said books, records, accounts, and data in any manner whatever for four (4) years after the termination of this Contract.
3. Pursuant to California Government Code section 8546.7, the parties to this Contract shall be subject to the examination and audit of representative of the Auditor General of the State of California for a period of three (3) years after final payment under the contract. The examination and audit shall be confined to those matters connected with the performance of this contract including, but not limited to, the cost of administering the contract.

D. Clayton Act and Cartwright Act.

Section 7103.5 of the Public Contract Code specifies that in entering into a public works contract or a subcontract to supply goods, services or materials pursuant to a public works contract, the contractor or subcontractor offers and agrees to assign to the awarding body all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 commencing with Sec. 16700) of Part 2 of Division 7 of the Business and Professions Code, arising from purchase of goods, services or materials pursuant to the contract or subcontract. Pursuant to Public Contract Code section 7103.5, the Contractor and all of its subcontractors hereby offer and agree to assign to WVWD all rights, title, and interest in and to all causes of action they may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 commencing with Sec. 16700) of Part 2 of Division 7 of the Business and Professions Code, arising from purchase of goods, services or materials pursuant to this Agreement. This assignment shall become effective when WVWD tenders final payment to the Contractor without further acknowledgement by the parties.

E. Contractor Supervision.

The Contractor shall provide competent supervision and staffing of the Work as approved by WVWD. As necessary, the Contractor or designated representative shall be present at all times while work is actually in progress. Supervisor(s) must be able to proficiently speak, read and write in English.

F. Character of Workers.

If persons employed by the Contractor, including any subcontractors, shall appear to WVWD to be incompetent or to act in a disorderly or improper manner, he or she shall be discharged immediately on the request of WVWD, and such person shall not again be employed on the

Work.

G. Cooperation.

Should construction be under way by WVWD, other agencies or other contractors within or adjacent to the limits of the work specified or should work of any other nature be under way by other forces within or adjacent to said limits, the Contractor shall cooperate with all such other contractors or other forces to the end that any delay or hindrance to their work will be avoided. WVWD reserves the right to perform other or additional work at or near the site (including material sources) at any time, by the use of other forces.

H. Notices.

All notices permitted or required under this Contract shall be given at the following address, or at such other address as the parties may provide in writing for this purpose:

West Valley Water District:

855 W. Baseline Rd.
Rialto, CA 92377
Attn: John Thiel, P.E., General Manager

Dominguez General Engineering,

11096 Pipeline Avenue
Pomona, CA 91766
Alejandro Dominguez, Vice President

The parties may designate, in writing, other individuals to whom notice is to be given. Notices shall be deemed to be received upon personal delivery to the addresses above; if sent by overnight delivery, upon delivery as shown by delivery service records; if sent by facsimile, upon receipt as confirmed by the sending facsimile equipment; if by United States Postal Service, five days after deposit in the mail.

SECTION 19 – FEDERAL CONTRACT REQUIREMENTS

The contract agreement must include all applicable clauses stipulated at 2 CFR § 200.327 and Appendix II. See General Conditions Section 3.39.10 “Procurement Requirements for the EPA Community Grants Program” for further information. The Contract Documents including the applicable clauses and following exhibits are additional provisions that are incorporated into this Agreement and are binding. Any provisions in EXHIBIT A–EPA GENERAL TERMS AND CONDITIONS, EFFECTIVE OCTOBER 1, 2025; EXHIBIT B–GOVERNMENT GRANT PROVISIONS; EXHIBIT C–DAVIS-BACON REQUIREMENTS; EXHIBIT D – MITIGATION MONITORING AND REPORTING PROGRAM, EXHIBIT E – PROGRAMMATIC CONDITIONS & CROSS-CUTTERS, and EXHIBIT F – STATE PREVAILING WAGE DETERMINATION that are not applicable to Contractor or its subcontractors is considered self-deleting. In the event of conflicting provisions, the order of precedence shall be in the following order:

1. Agreement
2. Attachments
3. Contract Document for the Construction of ZONE 2 WATERLINE AND SERVICE RELOCATION IN THE BLOOMINGTON AREA, 7TH STREET, 9TH STREET, LINDEN AVENUE AND CEDAR AVENUE – PHASE IIIB (W25036)
4. Addenda
5. EXHIBIT A – EPA GENERAL TERMS AND CONDITIONS, EFFECTIVE OCTOBER 1, 2025
6. EXHIBIT B – GOVERNMENT GRANT PROVISIONS
7. EXHIBIT C – DAVIS-BACON REQUIREMENTS DOL WAGES **CA20260026** AS OF **5/18/2026**
8. EXHIBIT D – MITIGATION MONITORING AND REPORTING PROGRAM
9. EXHIBIT E – PROGRAMMATIC CONDITIONS & CROSS-CUTTERS
10. EXHIBIT F – STATE PREVAILING WAGE DETERMINATION

IN WITNESS WHEREOF, the parties hereto have caused this contract to be executed on the day and year first above written.

WEST VALLEY WATER DISTRICT

By: _____

Printed Name: Kelvin Moore

Title: President, Board of Directors

Dated: _____

By: _____

Printed Name: John Thiel, P.E.

Title: General Manager

Dated: _____

**DOMINGUEZ GENERAL ENGINEERING,
INC.**

By: _____

(Authorized Representative of Contractor)

Printed Name: Alejandro Dominguez

Title: Vice President

(Attach Acknowledgment for Authorized
Representative of Contractor)

Dated: _____

License No.: 814046

ATTACHMENT A

INSURANCE

ATTACHMENT B

DESIGNATION OF SUBCONTRACTORS

ATTACHMENT C

PUBLIC WORKS CONTRACTOR REGISTRATION CERTIFICATION

PUBLIC WORKS CONTRACTOR REGISTRATION CERTIFICATION

Pursuant to Labor Code sections 1725.5 and 1771.1, all contractors and subcontractors that wish to bid on, be listed in a bid proposal, or enter into a contract to perform public work must be registered with the Department of Industrial Relations. See <https://www.dir.ca.gov/PublicWorks/PublicWorks.html> for additional information.

No bid will be accepted nor any contract entered into without proof of the contractor's and subcontractors' current registration with the Department of Industrial Relations to perform public work.

Contractor hereby certifies that it is aware of the registration requirements set forth in Labor Code sections 1725.5 and 1771.1 and is currently registered as a contractor with the Department of Industrial Relations.

Name of Contractor: Dominguez General Engineering, Inc.

DIR Registration Number: 1000006121

Contractor further acknowledges:

1. Contractor shall maintain a current DIR registration for the duration of the project.
2. Contractor shall include the requirements of Labor Code sections 1725.5 and 1771.1 in its contract with subcontractors and ensure that all subcontractors are registered at the time of bid opening and maintain registration status for the duration of the project.
3. Failure to submit this form or comply with any of the above requirements may result in a finding that the bid is non-responsive.

Name of Contractor DOMINGUEZ GENERAL ENGINEERING, INC.

Signature _____

Name and Title Alejandro Dominguez, Vice-President

Dated _____

ATTACHMENT D

CONTRACTOR'S PROPOSAL

ATTACHMENT E

BOND FORMS

EXHIBIT A – EPA GENERAL TERMS AND CONDITIONS

EXHIBIT B – GOVERNMENT GRANT PROVISIONS

EXHIBIT C – DAVIS-BACON REQUIREMENTS DOL PREVAILING WAGE DETERMINATION

US DEPARTMENT OF LABOR PREVAILING WAGE DETERMINATIONS HAVE BEEN PROVIDED FOR CONVENIENCE
AND CAN BE FOUND ON THE WEBSITE: [HTTPS://SAM.GOV/WAGE-DETERMINATIONS](https://sam.gov/wage-determinations)

EXHIBIT D – MITIGATION MONITORING AND REPORTING PROGRAM

**EXHIBIT E –
PROGRAMMATIC
CONDITIONS & CROSS-
CUTTERS**

EXHIBIT F – STATE PREVAILING WAGE DETERMINATION

STATE OF CALIFORNIA DIRECTOR'S GENERAL PREVAILING WAGE DETERMINATIONS HAVE BEEN PROVIDED
FOR MOST CRAFTS. ALL CRAFTS ARE FOUND ON THE WEBSITE:

[HTTPS://WWW.DIR.CA.GOV/OPRL/DPreWageDetermination.htm](https://www.dir.ca.gov/OPRL/DPreWageDetermination.htm)

EXHIBIT B

TASK ORDER NO. 6

Construction Management and Inspection Services for the W25036 Bloomington Area Waterline Replacement Project Phase 3B

This Task Order ("Task Order") is executed this _____ day of _____, 2026 by and between West Valley Water District, a public agency of the State of California ("District") and Albert A. Webb Associates ("Consultant").

RECITALS

- A. On or about **February 20, 2025** 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 provided 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 and this Task Order, 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**

By _____
John Thiel, General Manager

CONSULTANT:

ALBERT A. WEBB ASSOCIATES

By  _____

Name Reed Chilton

Its Director

EXHIBIT “1”

TO

TASK ORDER NO. 6

SCOPE OF SERVICES

The purpose of the scope of services is outlined in the attached proposal dated June 16, 2026 which states the tasks that are necessary for construction management and inspection services as it relates to the subject project.

Natalie Avila
Project Manager
West Valley Water District (WVWD)
855 W. Base Line Rd. | Rialto, CA 92377

June 16, 2026

RE: Proposal for Construction Management and Inspection Services for the W25036 Bloomington Area Waterline Replacement Project Phase 3B

Dear Natalie,

Webb Associates is pleased to provide you with this proposal for Construction Management and Inspection services for the subject project referenced above. Enclosed you will find our Project Understanding (Section 1), Scope of Work (Section 2), and Compensation for Services (Section 3) for your review and consideration.

If you find this proposal acceptable, please notify our office so a contract agreement can be prepared. We appreciate this opportunity to be of service and look forward to hearing from you. If you have any questions regarding this proposal, please contact us at 951-830-5746.

Sincerely,

ALBERT A. WEBB ASSOCIATES



Reed Chilton, P.E.
Director of Construction Management and Inspection

SECTION 1 - PROJECT UNDERSTANDING

1.1 PROJECT DETAILS

- **Construction Duration:** 240 Working Days
- **Location:** 9th Street from Locust Avenue to Linden Avenue, Linden Avenue from 7th Street to 9th Street, 7th Street from Elm Avenue to Cedar Avenue, and Cedar Avenue from 7th Street to 9th Street
- **Project Description:** The project involves the construction of a new Cement Mortar Lined and Coated (CML&C) steel water main along with all necessary appurtenances and services to replace the existing pipeline. Additionally, the project includes roadway restoration, encompassing pavement repair, signing and striping, and traffic signal loop replacement. The construction phase is in part funded by an EPA grant and will be subject to federal labor compliance and reporting by the contractor.
- **Project Plans:** Zone 2 Waterline and Service Relocation Phase 3B dated May 2026
- **Level of Involvement:** Based on discussions and coordination with the District, Construction Management and Inspection services are being requested on a limited basis. It is assumed that the District will be providing primary inspection and construction management services for the project. The scope and level of involvement outlined in this proposal are less than what is typically provided. Therefore, it is understood that the services will be limited to the assumptions stated herein, and WEBB will not be providing a full-service scope.

1.2 PROJECT SCHEDULE

Duration	Description	Scope Required
8 Weeks	Pre-Construction meeting, Contracts, RFIs, Permits, Potholing	Construction Management
16 Weeks	Material Procurement	Construction Management (minimal)
20 Weeks	Progress bi-weekly meeting, Mobilization, Pipe Installation, Appurtenances, Testing, Pavement, and Street Restoration.	Construction Management (part-time) Part-Time Observation (up to 100 hours) Materials Testing (by others) Construction Survey
4 Weeks	Closeout Process, Punchlist, and As-builts	Construction Management

1.3 KEY PROJECT ISSUES:

1. Safety
 - a. The project is located in an existing neighborhood with no sidewalk and parking congestion
 - b. Proper notices are to be given to affected residents multiple times based on the Contractor's schedule
 - c. Existing utilities such as gas lines and energized utilities will be exposed during construction both in the public right-of-way and on private property
2. Unforeseen Conditions
 - a. Existing utilities in the work zone. Review plans with recent utility research and confirm the contractor potholes per the specifications and existing conditions.
 - b. Evaluate the Contractor's pothole report before construction begins, providing recommendations as needed.
3. Site Conditions
 - a. Review and verify lay sheets align with project plans and pothole findings to prevent misalignment issues. Contractor to order pipe materials only after the pothole report and lay sheets are finalized.
 - b. Review the Contractor's schedule and compare it to material lead times to maintain project timelines
 - c. Review preconstruction video to identify any pre-existing site conditions or damage before work begins. Itemize in a table format those potential damages will be anticipated to be in work zone and do not have specific bid items or callout notes on plans.
4. Compliance
 - a. District Standards
 - i. West Valley Water District's Standards and specifications for Domestic Water Facilities
 - b. County Standards
 - i. Permit requirements for road closures and excavation
 - ii. Discharge via De minimis permit
 - c. EPA / Federal requirements
 - i. BABA documentation
 - ii. AIS documentation
 - d. Pipe Chlorination and Testing
 - i. Review the Contractor's chlorination and flushing plan
 - ii. Verify proper discharge locations and confirm that all dechlorination measures

1.4 PROPOSED STAFF

WEBB has extensive experience in providing inspection and construction management services for complex water infrastructure projects, including the installation of new water mains and associated improvements. Our team is well-versed in overseeing the procurement and installation

W25036 Bloomington Area Waterline Replacement Project Phase 3B

of Cement Mortar Lined and Coated (CML/C) steel pipelines, ensuring compliance with industry standards and project specifications.

WEBB's construction management team works closely with WEBB's water resources team to ensure seamless coordination throughout the project. This collaboration allows us to address design considerations, optimize solutions, and proactively mitigate potential challenges.

With a strong focus on quality control, scheduling, and safety, WEBB effectively manages the installation of appurtenances, service connections, and fire hydrants. Our expertise extends beyond pipeline construction to include roadway restoration, where we oversee pavement repairs, signing and striping, and traffic signal loop replacements. By leveraging proactive coordination, thorough inspections, and clear communication, WEBB ensures successful project execution while minimizing disruptions to the surrounding community.

Construction Services Manager

Keith Barnett is a seasoned Construction Services Manager and Inspector at WEBB, with over 20 years of experience in construction management. Keith also has a background as a soils technician, which will allow him to provide valuable insight and ensure that the geotechnical firm selected has the best interests of the District in mind. His expertise spans a wide range of projects, particularly in waterline replacement, underground utilities, and street improvements.

Construction Manager

Andrew Vollrath will provide day-to-day construction management services and serve as the prime point of contact. He will be responsible for coordination with the District, Contractor, Inspector, materials testing, RFI's, submittals, scheduling, and change order reviews.

Inspection

The WEBB Inspector will communicate with the Construction Management Team and help coordinate the work in the field. The WEBB Inspector will prepare daily observation reports which will be shared with the District.

For budget purposes, WEBB inspection hours include up to 100 hours (4-hour daily minimum). Inspection will be schedule on an as-needed basis by the District.

SECTION 2 - SCOPE OF WORK

WEBB Associates (WEBB) will perform the following Scope of Construction Services for the Project. WEBB's scope and fee is based upon the anticipated project schedule and the direction provided by the District during the proposal process. In the event the Contractor exceeds the schedule, we will review the status of the work to determine the need for an increase in the budget amount. The assumptions included in the scope were used to determine the cost of each service. We are open to discuss the assumptions and will update the associated manhours, if necessary.

2.1 CONSTRUCTION MANAGEMENT

- Attend all meetings (up to 25 meetings)
- Verify schedule/pothole/layout comply
- Review and accept/respond to submittals (up to 25)
- Review and respond to RFIs (up to 10)
- Review and respond to field clarifications and ensure compliance with the Federal requirements (up to 5)
- Inspection on time and material basis (up to 100 hours) to monitor materials and methods in compliance with Contract Documents
- Ensure receipt of all BABA/AIS certifications for procured materials
- Assist with evaluating change order request and preparation of time and cost impact analysis as necessary (up to 10 CORs)
- Maintain redline plan consistent with contractor's actual work when providing inspection observations
- Prepare substantially complete notice at closeout
- Asbuilt

The District will provide the following Construction Management Services:

- Project Communication with all stakeholders
- Facilitate Pre-Construction meeting including minutes
- Review final Contractor Progress Payments
- Labor Compliance
- Federal Progress Reporting
- Facilitate Final Job Walk meeting

2.2 INSPECTION

- Provide limited oversight of the project on an as-needed basis determined by the District.
- Review the project specifications, special provisions, and bid documents.
- Provide Construction Inspection to monitor materials and methods for compliance with plans, specifications, and contract documents. Address and document nonconforming items as they are identified.
- Maintain daily reports on days on-site regarding construction activity, including progress, weather conditions, significant events which may affect the progress of the work and photographs.

- Review Contractor performance throughout the day and discuss discrepancies with the Contractor as they occur.
- Review soil compaction and materials testing.
- Maintain field files during construction, including a cumulative record of quantities constructed, daily reports, working day reports, change order documentation and digital images.
- Review and record final quantities.
- Provide recommendations for acceptance upon completion.
- Overtime inspection is not included in this proposal, but our inspector will be available for overtime hours if required by the Contractor. Overtime inspection will be billed at 1.5 times the standard billing rate. We assume that if overtime inspection is required, the anticipated budget will be exceeded. We would prepare a budget amendment request for the additional inspection hours.

2.3 CONSTRUCTION STAKING

Each staking task provided by WEBB will include the following:

- Provide coordination with the client and scheduling of field survey crews based on staking request received from the client. WEBB kindly requests 48-hour advance notice be provided for all staking requests.
- Provide office support to the field surveyors consisting of task setup, calculating, plotting, and preparation of grade sheets for items to be staked as requested by the client.
- Provide review and cataloging of all field staking and distribute digital grade sheets to client, for their use and distribution to agencies and/or contractors.
- NOTE: We do not anticipate any survey monuments to be distributed, therefore, we have not included any services to preserve or re-establish monuments.

2.3.1 Survey Control

- Establish and provide horizontal and vertical survey control points throughout the progress of the project including the setting of project Benchmarks.
- Provide horizontal and vertical survey control points throughout the progress of the project including the setting of project benchmarks.
- Provide GPS coordinates and files to Grader.

2.3.2 Waterline Stakes

- Domestic waterlines, consisting of stakes being set at 50-foot intervals offset from and graded to the flow line. Includes (BC's) beginning and (EC's) end of curves, PIs, VPIs, tees, casing limits, connections for services and appurtenances.
- Domestic appurtenances, consisting of two stakes for each hot tap, fire hydrant, water meter, blow-off, and air vac. First stake for actual location, second stake for offset and grade.

The total budget outlined within this scope of work is based on a total of 11 mobilizations, any mobilizations beyond this amount will be billed on a Time and Materials (T&M) basis in addition to the amounts provided in our compensation for services. It is acknowledged

that the client or client representative will give Albert A. WEBB Associates a minimum of 48-hour advance notice, together with a minimum of 4 (four) hours of construction staking work per day for all construction staking requests. Re-stake request will be addressed by a Time and Materials (T&M) ticket based on a 4 (four) hour minimum, unless previously agreed to in writing. Staking request cancelled with less than 24-hour advance notice are subject to a 4 (four) hour minimum field crew charge.

2.4 ADDITIONAL SERVICES

Services which are not specifically identified herein as services to be performed by WEBB Associates are considered Additional Services for the purposes of this Proposal. The District may request that WEBB Associates perform services which are Additional Services. WEBB Associates will perform such additional services upon execution of an amendment to this Agreement setting forth the scope, schedule, and fee for such additional services.

2.5 EXCLUSIONS

Any work relating to the following is specifically excluded for the Construction Services proposed herein and, if required, must be contracted for under a separate contract or as an addendum to this contract:

- Full-time inspection
- Full-service Construction Management
- Welding Inspection
- Survey monument preservation and re-establishment
- Utility Potholing
- Soil and Material Testing
- Prepare Storm Water Pollution Prevention Plans (SWPPP)
- Permit and Payments
- Traffic Control Plans (by Contractor)
- Utility Relocation Plans
- Property Acquisition
- Any other work task not specifically in the Scope of Services.
- Operational Plan
- O & M Manuals

This proposal is based in part on the assumption that the District acknowledges that WEBB Associates is not responsible for the performance of work by third parties. Notwithstanding any other language contained herein, WEBB Associates, and its officers, directors, and employees, shall not be liable except to the extent that any Project damages are directly attributable to the actions of WEBB Associates.

EXHIBIT “2”
TO
TASK ORDER NO. 6

COMPENSATION

Task	Description	Cost
1	Construction Management	\$99,400.00
2	Inspection	\$17,400.00
3	Construction Staking	\$44,300.00
	Grand Total	\$161,100.00

SECTION 3 - COMPENSATION FOR SERVICES

3.1 FEE SUMMARY

WEBB is committed to providing services in a skillful, professional and competent manner consistent with the industry standards, practices and principles generally recognized as being employed by professionals in the same discipline in the County of San Bernardino and the State of California. Fees are listed below associated with the scope of work. Based upon the project's scope of work, a summary of WEBB's construction services budget is as follows:

Work shall be billed on a time and materials basis not to exceed the amount indicated below without prior authorization from the client. Total fees for services shown in the Scope of Work (Exhibit "B") shall be **\$161,100**. A breakdown of our fees is listed below:

Item No.	Description	Fee
1	Construction Management	\$99,400
2	Inspection	\$17,400
3	Construction Staking	\$44,300
TOTAL		\$161,100

This proposal and budget are valid for 60 days from date of proposal.

Task budgets are estimates and may be used interchangeably as needed but not to exceed the budget total. Any additional services requested outside this scope will be provided under separate contract addenda for additional fees. Invoices will be submitted monthly based on the percentage of work completed. All invoices shall be due and payable upon receipt. If invoices remain unpaid after 30 days, work on project may cease and interest of 1.5% per month shall be charged on unpaid balances.

Charges for printing, copying, mileage, postage, outside services, and for coordination or other services not specifically listed in the scope of work, will be billed on a time and material basis, in accordance with our Schedule of Fees as Reimbursable Expenses. Checking and/or filing fees are not included in this contract and shall be paid by the client directly to the appropriate governmental agency.

Costs for custom invoicing, if desired by the client, shall be negotiated prior to commencement of work.

Fee Schedule 2025

CLASSIFICATION

<u>Engineers/Project Managers/Planners/Scientists/ Assessment/Special Tax Consultants/Landscape Architects/Designers</u>	<u>Rates \$/Hour</u>
Principal II	331.00
Principal I	316.00
Senior III	300.00
Senior II	286.00
Senior I	276.00
Associate III	257.00
Associate II	245.00
Associate I	232.00
Assistant V	210.00
Assistant IV	187.00
Assistant III	173.00
Assistant II	156.00
Assistant I	138.00

Survey Services

3-Person Survey Party	457.00
2-Person Survey Party	356.00
1-Person Survey Party	255.00

Inspection Services

Construction Manager III	294.00
Construction Manager II	260.00
Construction Manager	210.00
Inspector (Non-Prevailing Wage)	154.00
Inspector Overtime (Non-Prevailing Wage)	205.00
Inspector (Prevailing Wage)	166.00
Inspector Overtime (Prevailing Wage)	220.00

Administrative Services

Project Coordinator	150.00
Administrative Assistant III	127.00
Administrative Assistant II	114.00
Administrative Assistant I	91.00

Other Direct Expenses

Incidental Charges	Cost + 15%
Postage	Cost
Subcontracted Services	Cost + 15%
Survey/Inspection Per Diem	Prevailing Wage Rate
In-House Delivery Up to 1/2 hour	38.00
In-House Delivery 1/2 Hour up to 1 Hour	73.00
In-House Delivery Over 1 Hour up to 2 Hours	136.00
In-House Delivery Over 2 Hours	193.00
Survey/Inspection Vehicle	0.90/Mile
Mileage	0.82/Mile



Fee Schedule 2025

Note: All rates are subject to change based on annual inflation and cost of living adjustments. Prevailing wages are dictated by the California Department of Industrial Relations (DIR). As such, the indicated rate will remain in effect until revised rates are published by the DIR. The rate shown shall be subject to renegotiation to remain in compliance with State requirements if prevailing wages are increased by the DIR.

** **A FINANCE CHARGE** of 1 ½ % per month (18% per year) will be added to any unpaid amount commencing thirty (30) days from invoice date. A mechanic's lien may be filed for any invoice remaining unpaid after thirty (30) days from invoice date.*

EXHIBIT “3”
TO
TASK ORDER NO. 6
SCHEDULE

Schedule to be determined by District staff.



STAFF REPORT

DATE: September 1, 2026

TO: Engineering, Operations and Planning Committee

FROM: Joanne Chan, Director of Operations

SUBJECT: Approve Second Amendment to Reimbursement Agreement with San Bernardino Valley Municipal Water District for Hidden Valley Wetlands Mitigation Project

STRATEGIC GOAL:

Strategic Goal 4 - Strengthen Partnerships with Outside Agencies; A. Engage in Regional Projects, Advocacy, and Grant Pursuits

MEETING HISTORY:

None.

BACKGROUND:

In May 2016, the West Valley Water District (District) and the San Bernardino County Flood Control District (SBCFCD) executed an agreement permitting the spreading of water in Cactus Basin 2 in support of the District's Fluidized Bed Reactor (FBR) Groundwater Treatment project. Under the agreement, the District is responsible for obtaining all required regulatory permits and performing all maintenance activities associated with its water-spreading operations in Cactus Basin 2. This includes controlling any vectors and vegetation that may occur directly or indirectly as a result of the District's water-spreading activities.

The Streambed Alteration Agreement executed between the California Department of Fish and Wildlife (CDFW) and the District requires the District to provide compensatory mitigation for the loss of 12 acres of wetland and riparian habitat that has developed within Cactus Basin 2.

DISCUSSION:

In October 2020, the District partnered with the San Bernardino Valley Municipal Water District (SBVMWD) to coordinate the development and implementation of the required mitigation project at Hidden Valley Wetlands in Riverside County.

SBVMWD serves as the lead agency for project planning, implementation, and compliance reporting. The Hidden Valley Wetlands mitigation project encompasses approximately 85 acres. The District's mitigation obligation associated with Cactus Basin 2 is 12 acres.

Pursuant to the parties' agreement, the District's proportionate share of the mitigation costs at Hidden Valley Wetlands will be based on the ratio of the District's 12-acre mitigation obligation to the total 85-acre mitigation project acreage.

The District has no land acquisition costs associated with the mitigation project. The estimated cost of habitat management activities for the District's 12-acre mitigation area over the next 12 months is \$40,000. SBVMWD staff will reassess the level of effort required toward the end of spring 2027 to determine the anticipated management needs and costs for the subsequent 12-month period.

District staff has worked closely with SBVMWD staff to develop the Reimbursement Agreement between the parties, attached hereto as **Exhibit A**.

FISCAL IMPACT:

The costs associated with the District's mitigation obligations are fully reimbursable. Raytheon Technologies will reimburse the District for the full cost of the mitigation activities. The District's estimated mitigation and habitat management costs for the current fiscal year are approximately \$40,000.

REQUESTED ACTION:

Recommends that the Committee forward a recommendation to the Board of Directors to:

1. Approve the Second Amendment to the Reimbursement Agreement with San Bernardino Valley Municipal Water District; and
2. Authorize the General Manager to execute all necessary documents.

Attachments

[Exhibit A - Second Amendment to Reimbursement Agreement.pdf](#)

EXHIBIT A

SECOND AMENDMENT TO REIMBURSEMENT AGREEMENT

THIS SECOND AMENDMENT TO REIMBURSEMENT AGREEMENT (“*Second Amendment*”) is entered into and effective as of July 1, 2026 (“*Second Amendment Effective Date*”), by and between WEST VALLEY WATER DISTRICT, a county water district organized and operating pursuant to California Water Code section 30000 *et seq.* (“*WVWD*”), and SAN BERNARDINO VALLEY MUNICIPAL WATER DISTRICT, a municipal water district organized and operating pursuant to California Water Code section 71000 *et seq.* (“*SAN BERNARDINO VALLEY*”). WVWD and SAN BERNARDINO VALLEY are sometimes referred to herein individually as “*Party*” and collectively as “*Parties*”.

RECITALS

A. WVWD and SAN BERNARDINO VALLEY are parties to that certain Reimbursement Agreement, dated October 3, 2024, as amended by that certain First Amendment to Reimbursement Agreement, dated April 1, 2025 (as amended, “*Reimbursement Agreement*”), with respect to a framework to reimburse SAN BERNARDINO VALLEY for expenses incurred in implementing habitat management actions associated with the HMMP for the SAA at HVWA, as defined in the Reimbursement Agreement.

B. The term of the Reimbursement Agreement expired on June 30, 2026.

C. On or about July 8, 2026, SAN BERNARDINO VALLEY received a cost estimate from the Santa Ana Watershed Association (“*SAWA*”) for additional habitat management actions within WVWD’s 12-acre habitat management area at HVWA through June 30, 2027. The estimated cost of such additional habitat management actions is Forty Thousand Dollars and Zero Cents (\$40,000.00), as identified in the Scope and Cost Estimate for Lower Cactus Basin #2 Mitigation Area attached as *Exhibit 2* hereto and incorporated herein by reference.

D. The Parties wish to establish and agree to a framework to reimburse SAN BERNARDINO VALLEY for expenses incurred in implementing the additional habitat management actions associated with the HMMP for the SAA at WVWD’s 12-acre mitigation area at HVWA through June 30, 2027, as identified in *Exhibit 2* attached hereto, upon the terms and conditions set forth in this Second Amendment.

NOW THEREFORE, in consideration of the matters recited and the mutual promises, covenants, and conditions set forth in this Second Amendment, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

OPERATIVE PROVISIONS

1. Incorporation of Recitals. Each and every one of the Recitals set forth above is a material part of this Second Amendment and is hereby incorporated by reference into and made part of this Second Amendment by this reference.

2. Definitions. Defined terms not otherwise defined in this Second Amendment shall have the meanings ascribed thereto in the Reimbursement Agreement.

3. Reinstatement; Extension of Term. Notwithstanding the actual date of execution of this Second Amendment, the Parties desire and intend to reinstate the Reimbursement Agreement in its entirety as of the Second Amendment Effective Date as if it had never expired, subject to the terms, conditions, and modifications set forth in this Second Amendment. The term of the Agreement is hereby extended through the earlier of: (a) June 30, 2027; or (b) SAN BERNARDINO VALLEY incurs total approved costs equaling the Maximum Reimbursement, as amended in this Second Amendment.

4. Maximum Reimbursement Increase. The Parties hereby increase the Maximum Reimbursement for implementation of WVWD's habitat management actions through June 30, 2027, by Forty Thousand Dollars (\$40,000.00), for a total Maximum Reimbursement of One Hundred Thirty-Five Thousand Eight Hundred Sixty-Two Dollars and Eighteen Cents (\$135,862.18).

5. HMMP Management and Implementation. The habitat management actions at WVWD's 12-acre mitigation area at HVWA to be managed and implemented by SAN BERNARDINO VALLEY pursuant to Section 2 of the Reimbursement Agreement are hereby deemed to include the additional habitat management actions identified in *Exhibit 2* attached to this Second Amendment.

6. Miscellaneous.

a. *Ratification.* Except as expressly modified by this Second Amendment, Parties acknowledge that the Reimbursement Agreement remains in full force and effect, enforceable in accordance with its terms.

b. *Conflicts.* To the extent that the Reimbursement Agreement conflicts with this Second Amendment, this Second Amendment shall prevail.

c. *Counterparts.* This Second Amendment may be executed in any number of counterparts, each of which shall be deemed an original and all of which when taken together shall constitute one and the same instrument. Signatures may be delivered electronically and shall be binding upon the Parties as if they were originals.

[Signature Page Follows]

IN WITNESS WHEREOF, the Parties have executed this Second Amendment as of the Second Amendment Effective Date.

**SAN BERNARDINO VALLEY
MUNICIPAL WATER DISTRICT**

By: _____
Heather P. Dyer
CEO/General Manager

WEST VALLEY WATER DISTRICT

By: _____
John Thiel
General Manager

EXHIBIT 2

SAWA SCOPE AND COST ESTIMATE FOR LOWER CACTUS BASIN #2 MITIGATION AREA



5029 La Mart Drive, Suite E
Riverside, CA 92507
(951) 780-1012
Fax (951) 780-5893
<http://www.sawatershed.org>

Board of Directors:

Brett Mills,
Chair

Kerwin Russell,
Vice-Chair

Mandy Parkes,
Treasurer

David McMichael,
Interim Secretary

Arturo Garcia,
Director

To: San Bernardino Valley Municipal Water District
Attn: Joanna Gibson
Subject: Scope and Cost Estimate for Lower Cactus Basin #2 Mitigation Area

Scope:

Non-native plant management on approximately 12-acres located at Hidden Valley Wildlife Area pursuant to the requirements of California Department of Fish and Wildlife, Lake and Streambed Alteration Agreement Number 1600-2018-0153-R6, for the Lower Cactus Basin 2 Maintenance Project (Revision 2).

Total cost from project start to 6-30-2027 is \$40,000.
Let me know if you have any questions,
Thank you,

Max Barrett
Interim Habitat Restoration Services Manager
mbarrett@sawatershed.org
(951) 388-0596



STAFF REPORT

DATE: September 1, 2026

TO: Engineering, Operations and Planning 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; A. Increase System Capacity for Anticipated Growth; E. Ensure Operational Continuity through Comprehensive Physical and Cybersecurity

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

MEETING HISTORY:

None.

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:

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 their 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

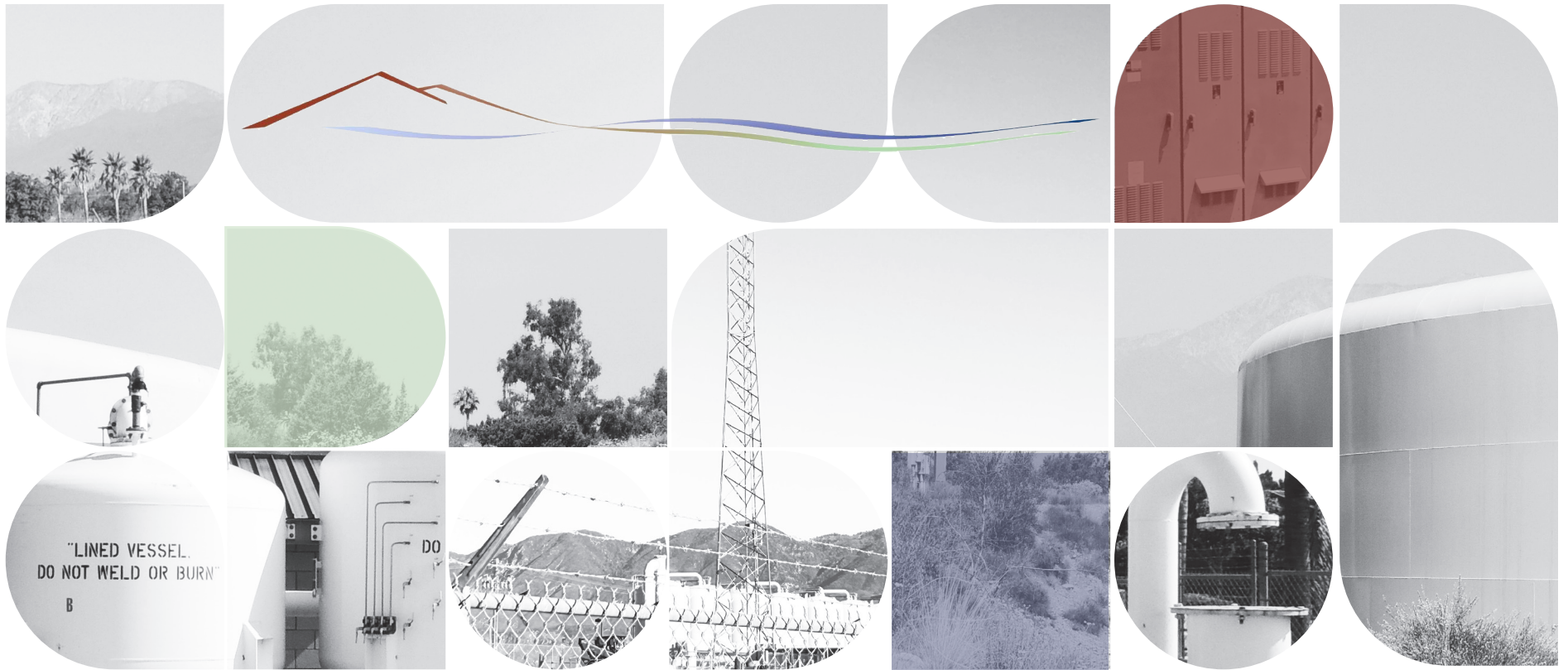
I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing Resolution No. 2026-15 was duly adopted by the Board of Directors of the West Valley Water District at a regular meeting held on September ____, 2026, by the following vote:

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 Documentation 79

9.1.6 S-6 SCADA Standard Documentation 79

9.2 Mid-Term Projects (M) 81

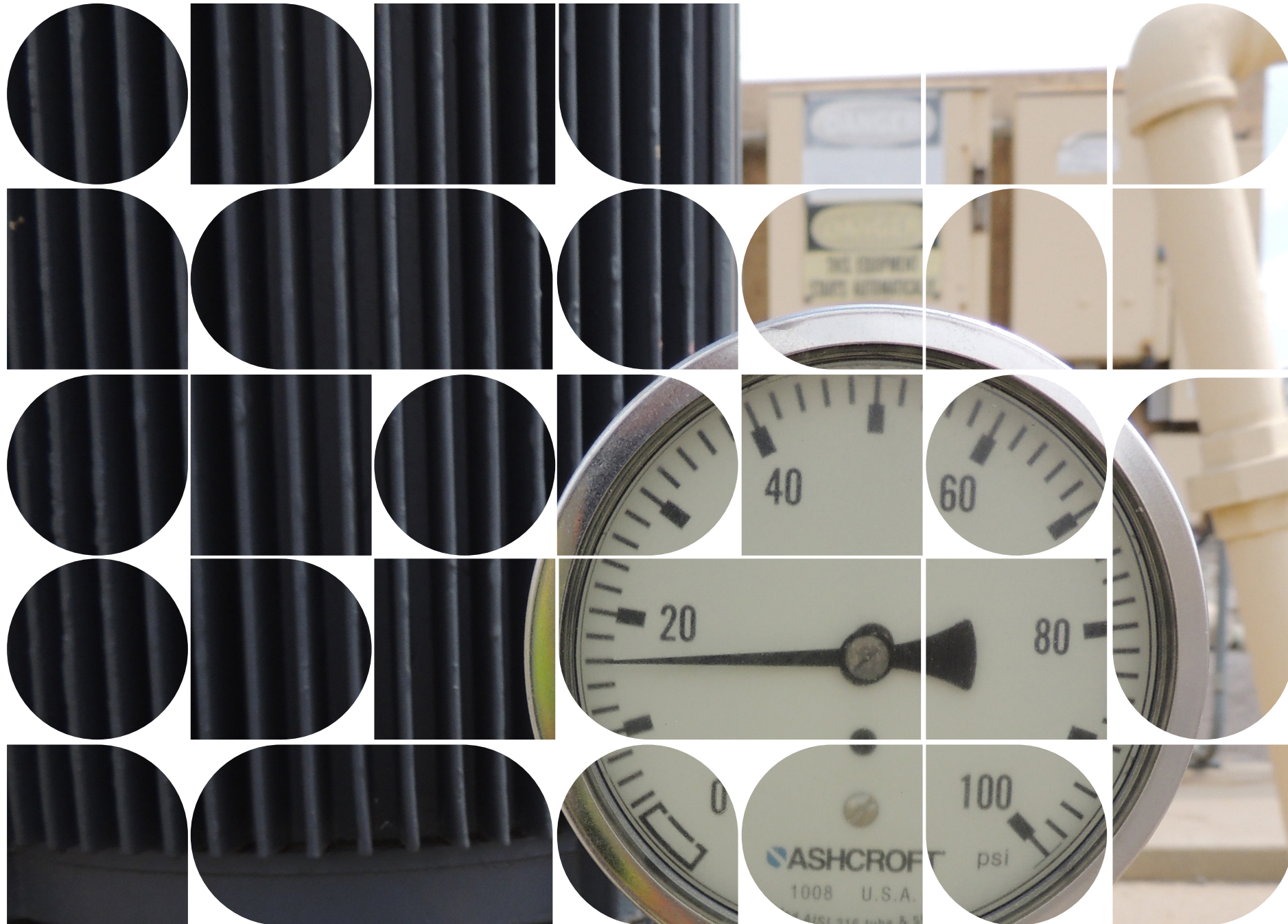
9.2.1 M-1 Cybersecurity Control Gap (Re)Assessment 81

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.

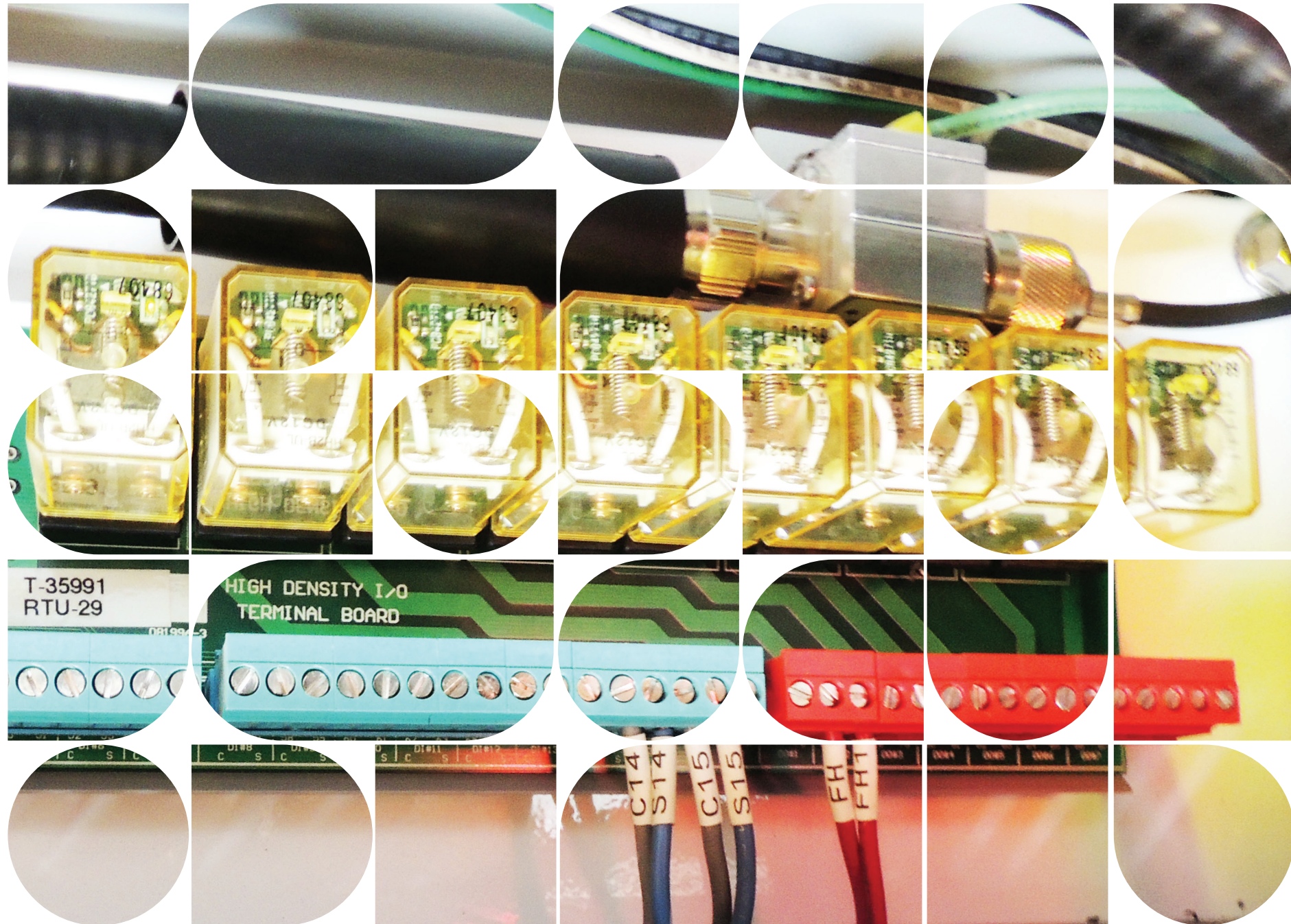
System Design Criteria – Establishes engineering and operational standards to guide future projects.

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.

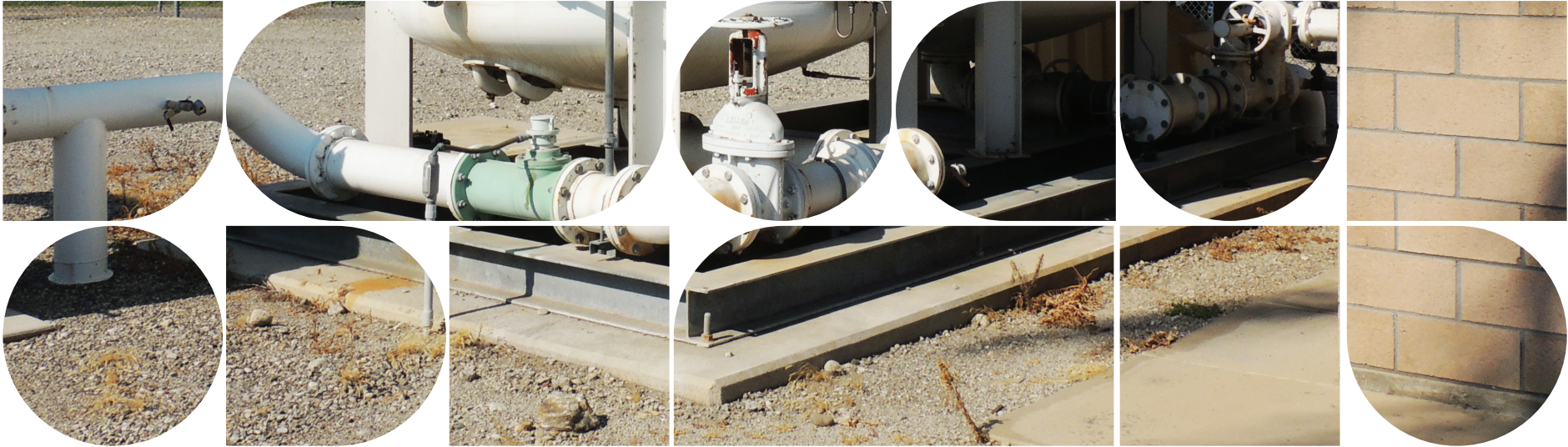
Beyond the project recommendations, this plan delivers a comprehensive set of system design criteria covering software standards, hardware standards, field enclosure standards, programming standards, and cybersecurity standards. These criteria provide the District with a consistent framework for evaluating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

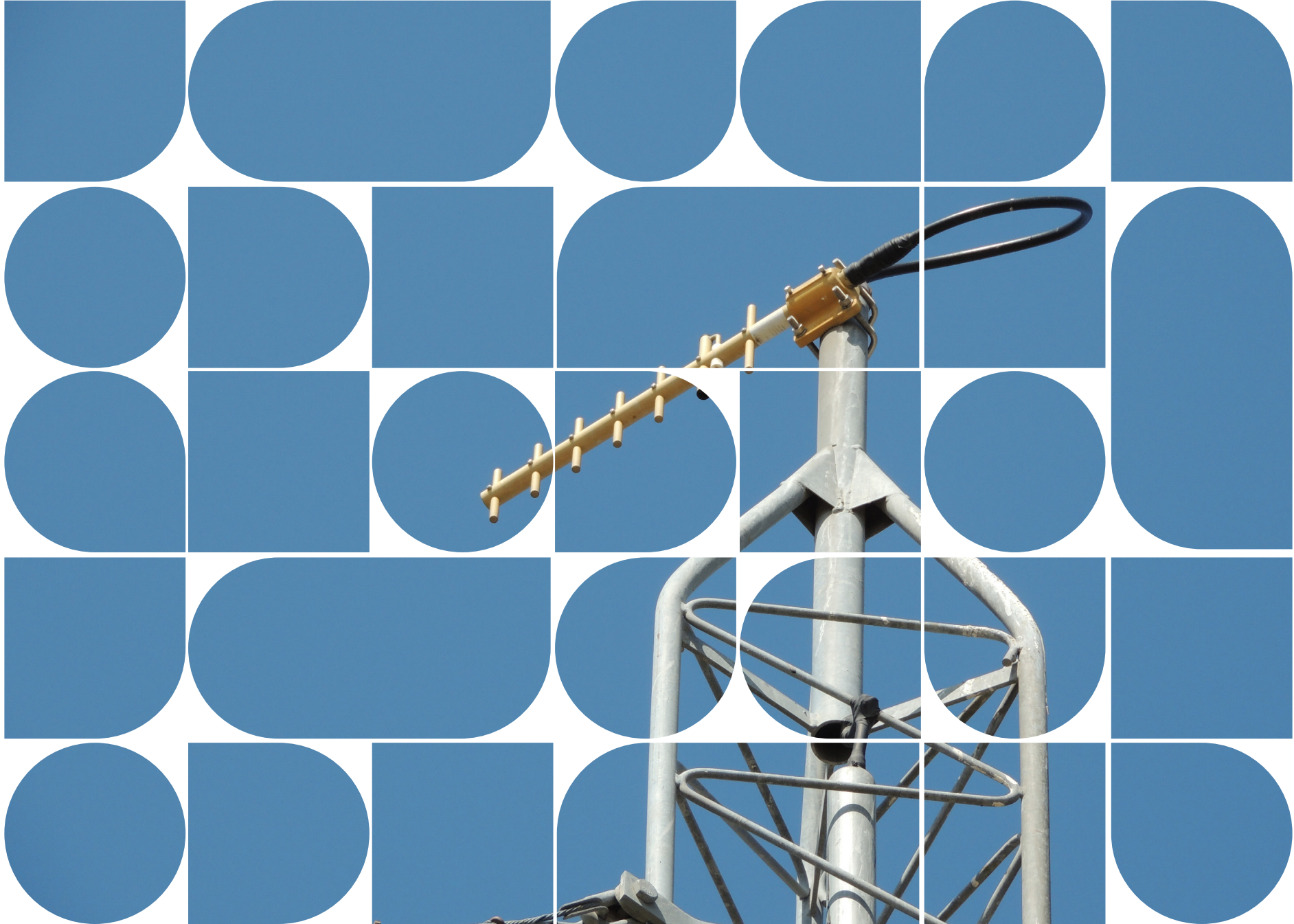
The HQ System runs on Wonderware InTouch with a Wonderware Historian, hosted on two standalone Dell PowerEdge hypervisors using a legacy version of VMware ESXi with no shared storage or automated failover. Despite the age of its computing and control components, the HQ System adheres to a moderately 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.

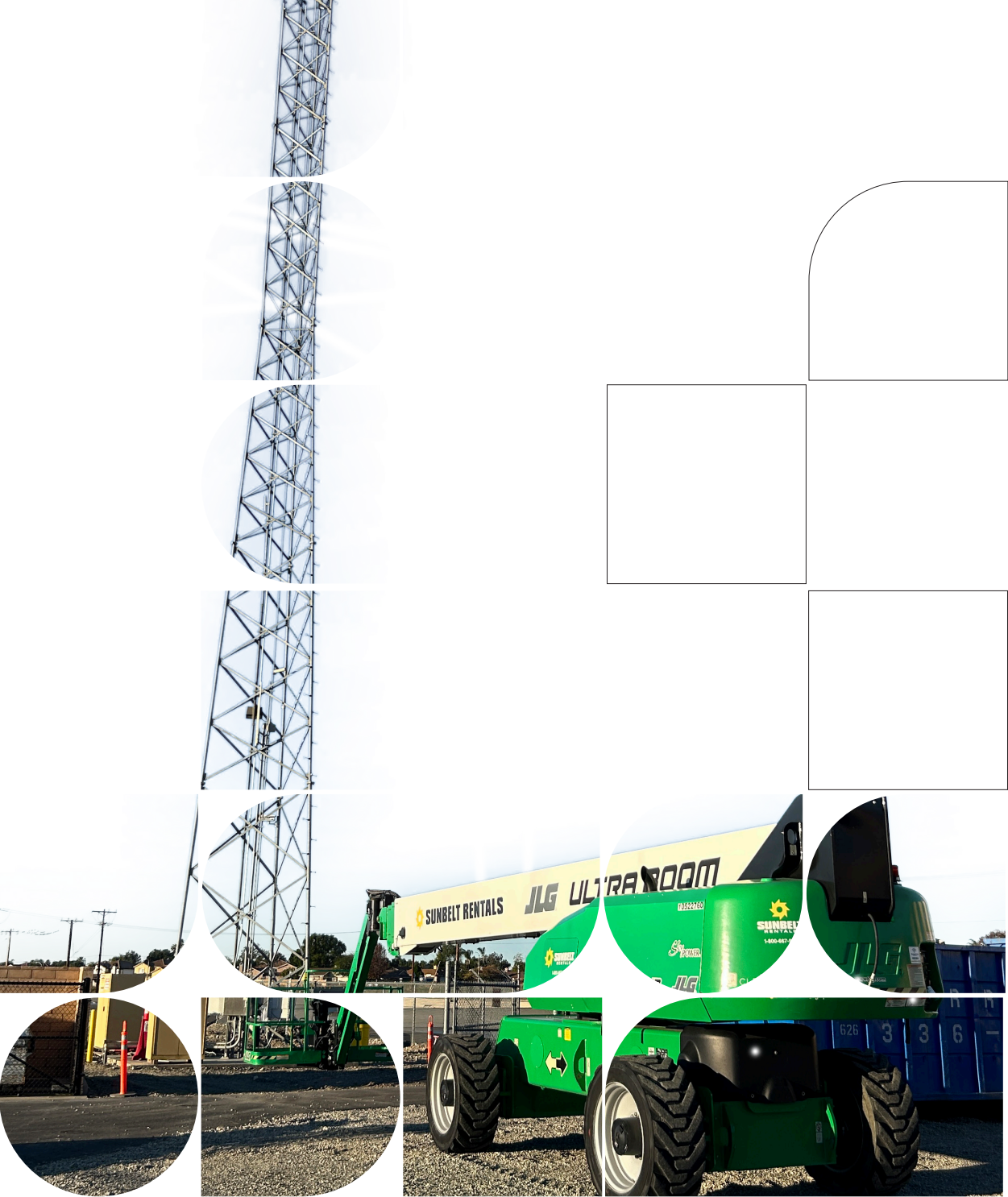
5.2.5.2 Programming Standards

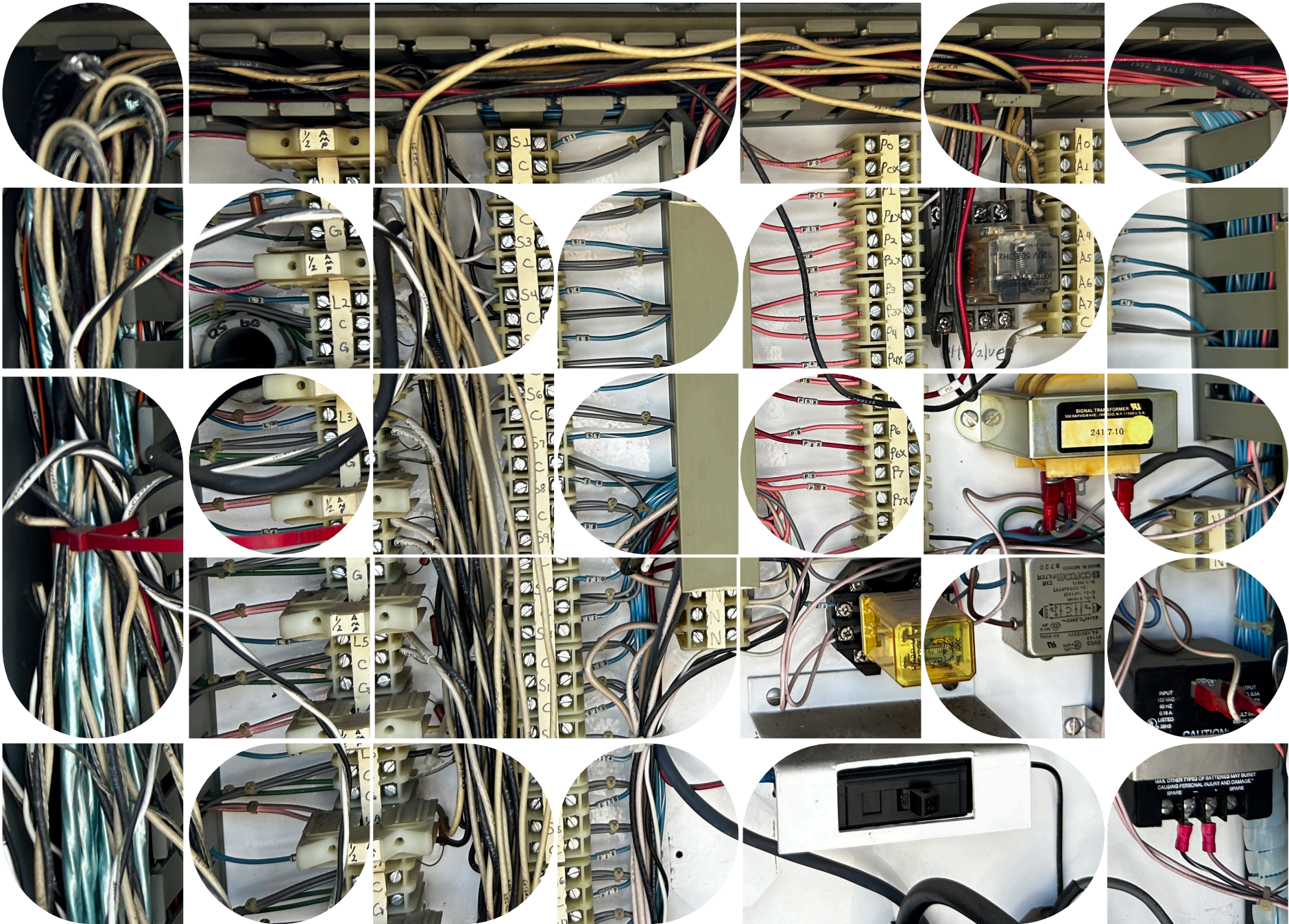
5.2.5.2.1 Code Structure, Tag Naming, and Documentation Requirements

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.

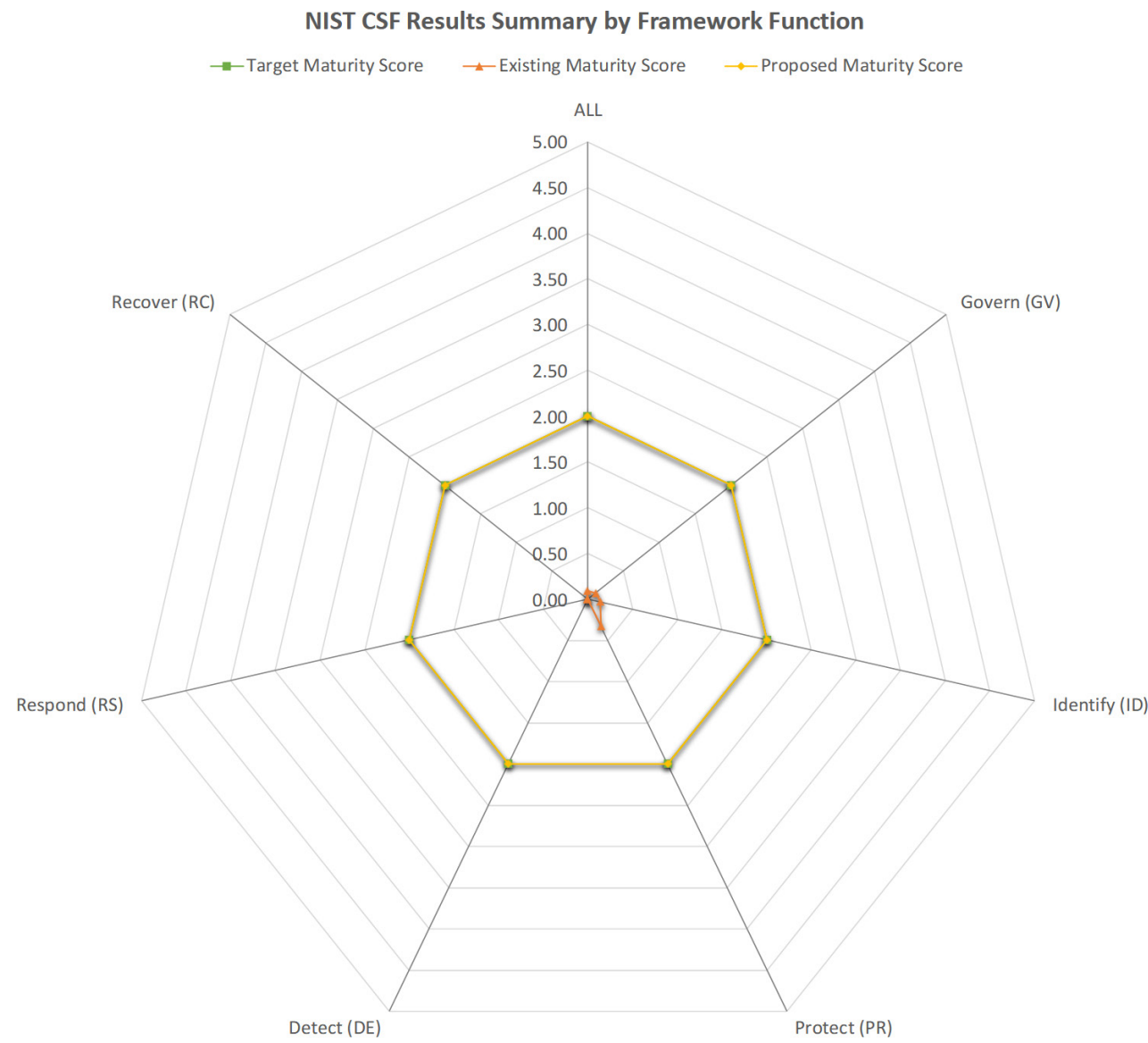
Framework Function Heat Map Table

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

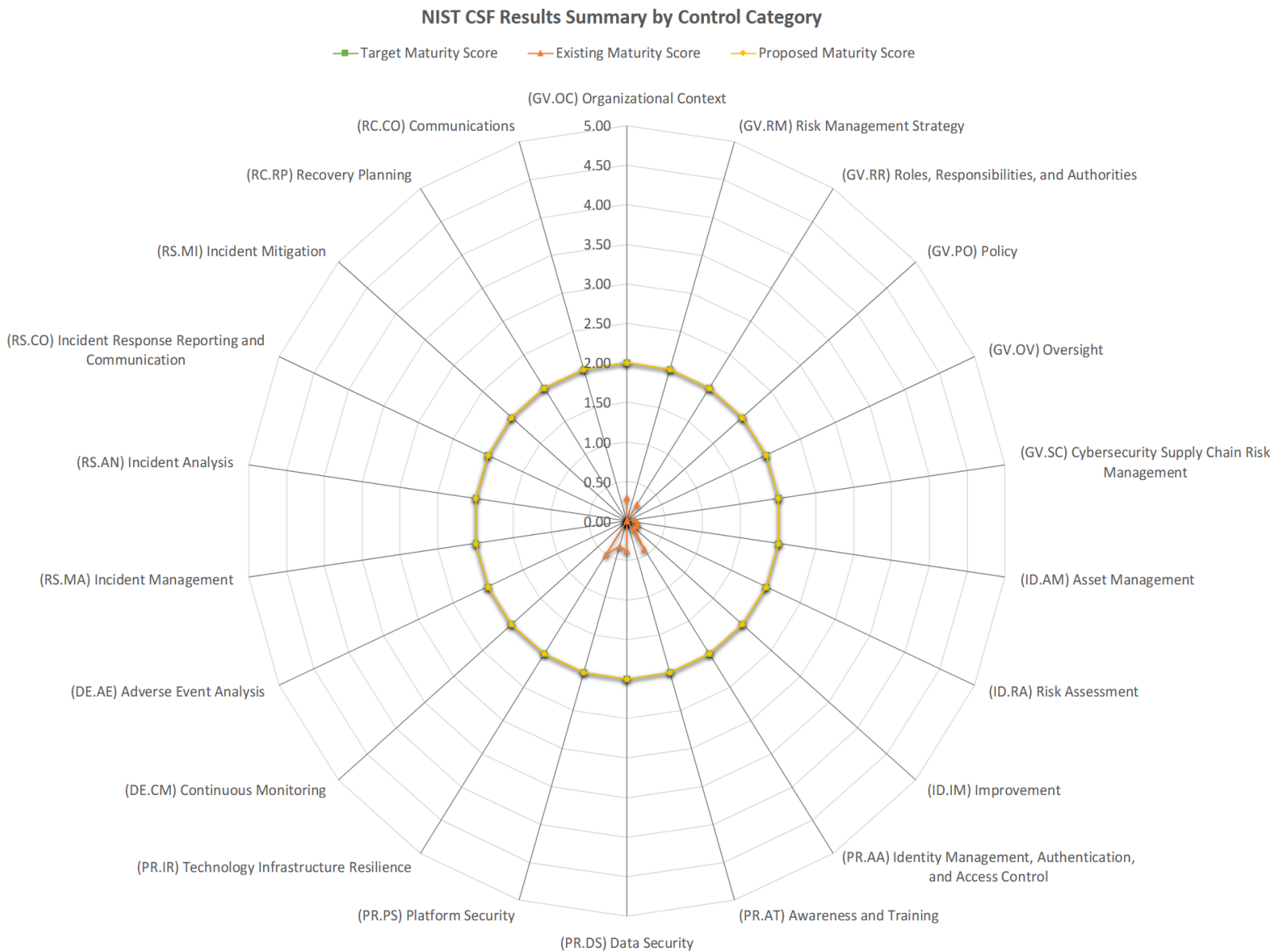
6.2.3 Maturity Level Results by Function

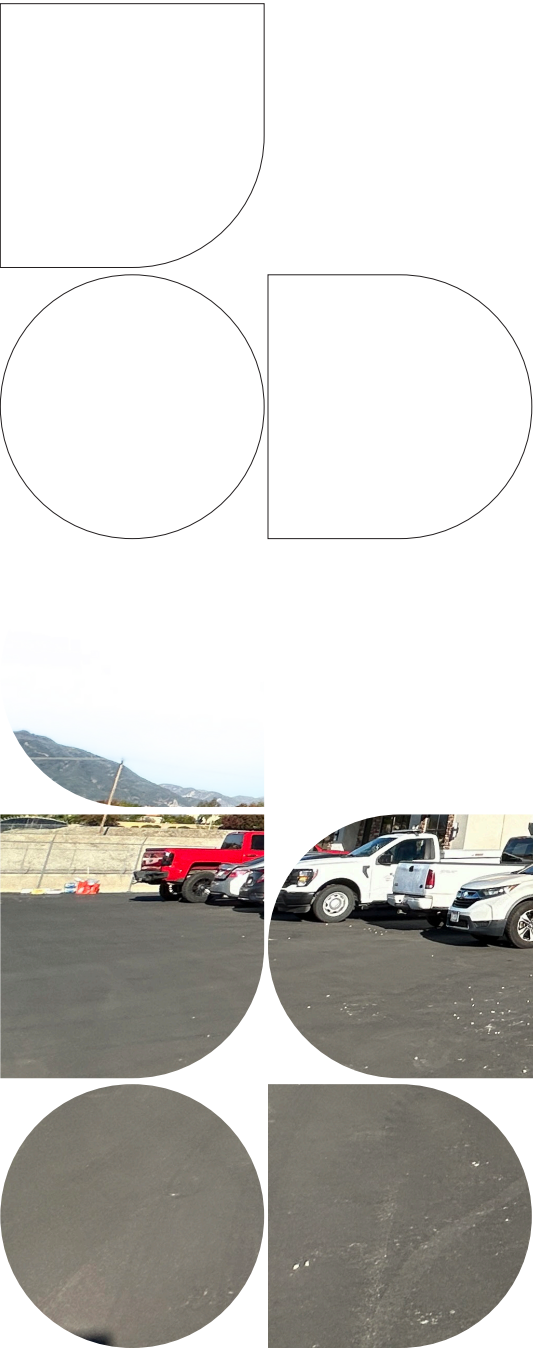
FIGURE 3 CYBERSECURITY MATURITY LEVEL RESULTS BY FUNCTION DIAGRAM



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

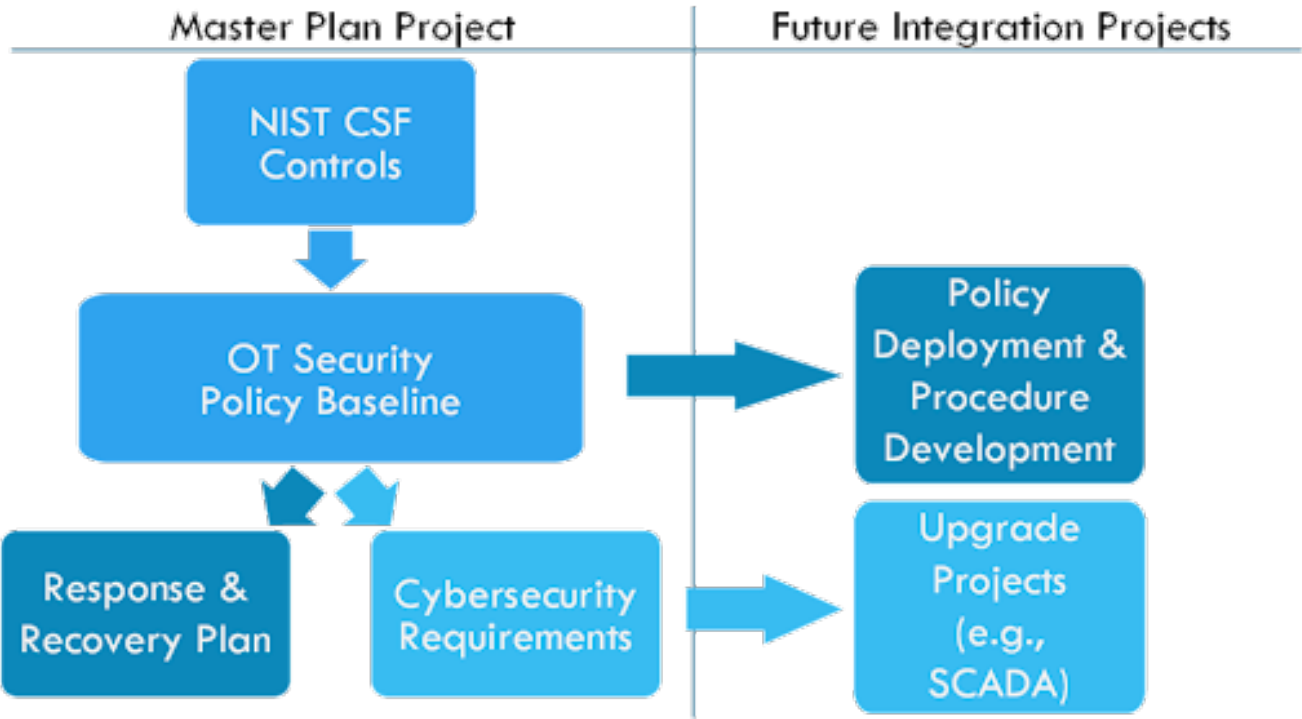
No formal incident response plan exists to guide internal or external reporting, escalation, or communication activities.	No formal incident recovery plan has been established to guide recovery activities following a cybersecurity incident.	and overseen by the District. The baseline policy was refined 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.
6.3.6.4 Incident Mitigation	6.3.7.2 Incident Recovery Communications	
No formal incident response plan has been established. Mitigation actions are handled on a case-by-case basis without documented procedures or defined roles.	No formal recovery plan exists to guide internal or external communications during or following recovery activities.	
6.3.7 Recovery Summary	6.4 BASELINE SECURITY POLICY	
6.3.7.1 Incident Recovery Plan Execution	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	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.

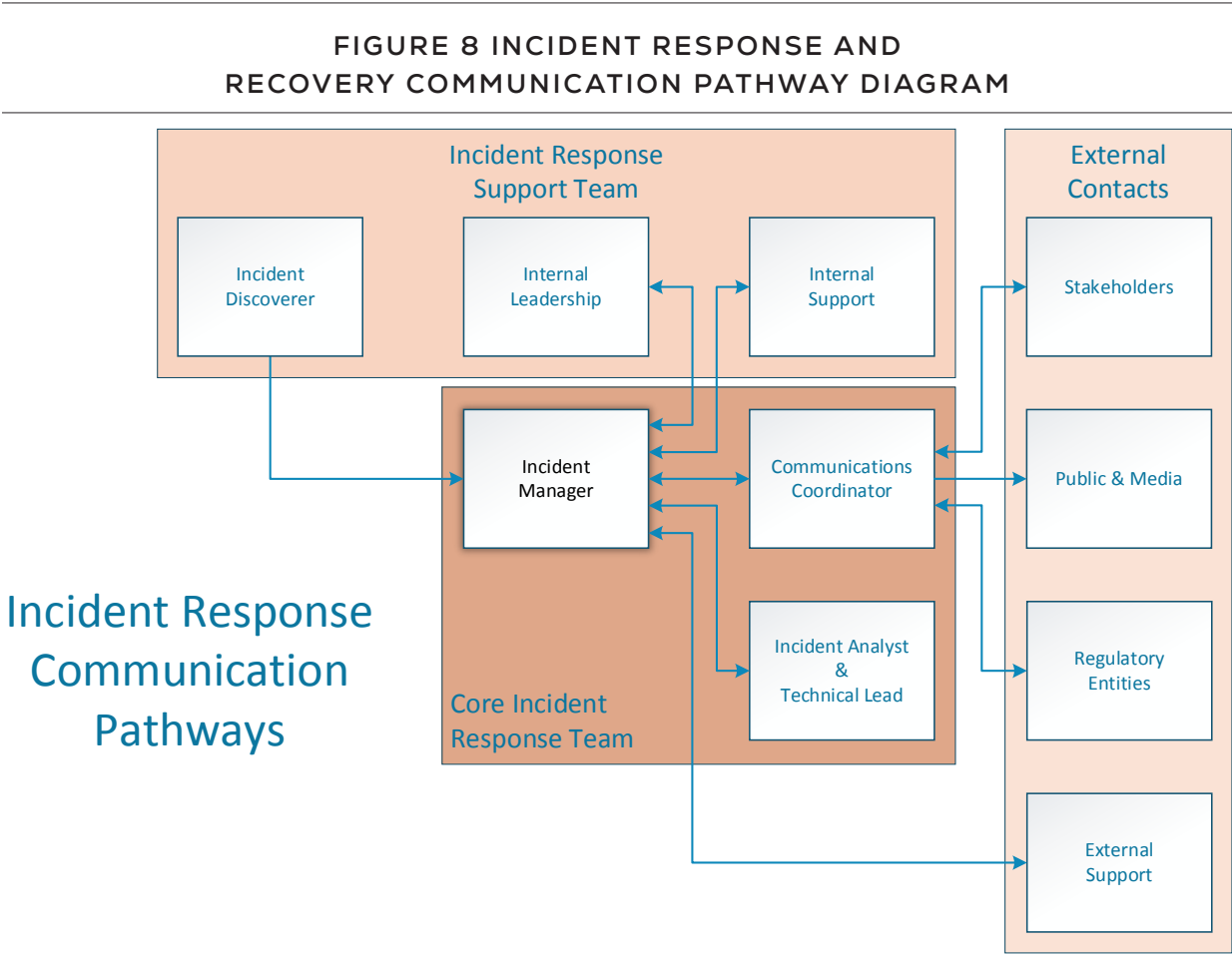
6.6 RESPONSE AND RECOVERY PLAN

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

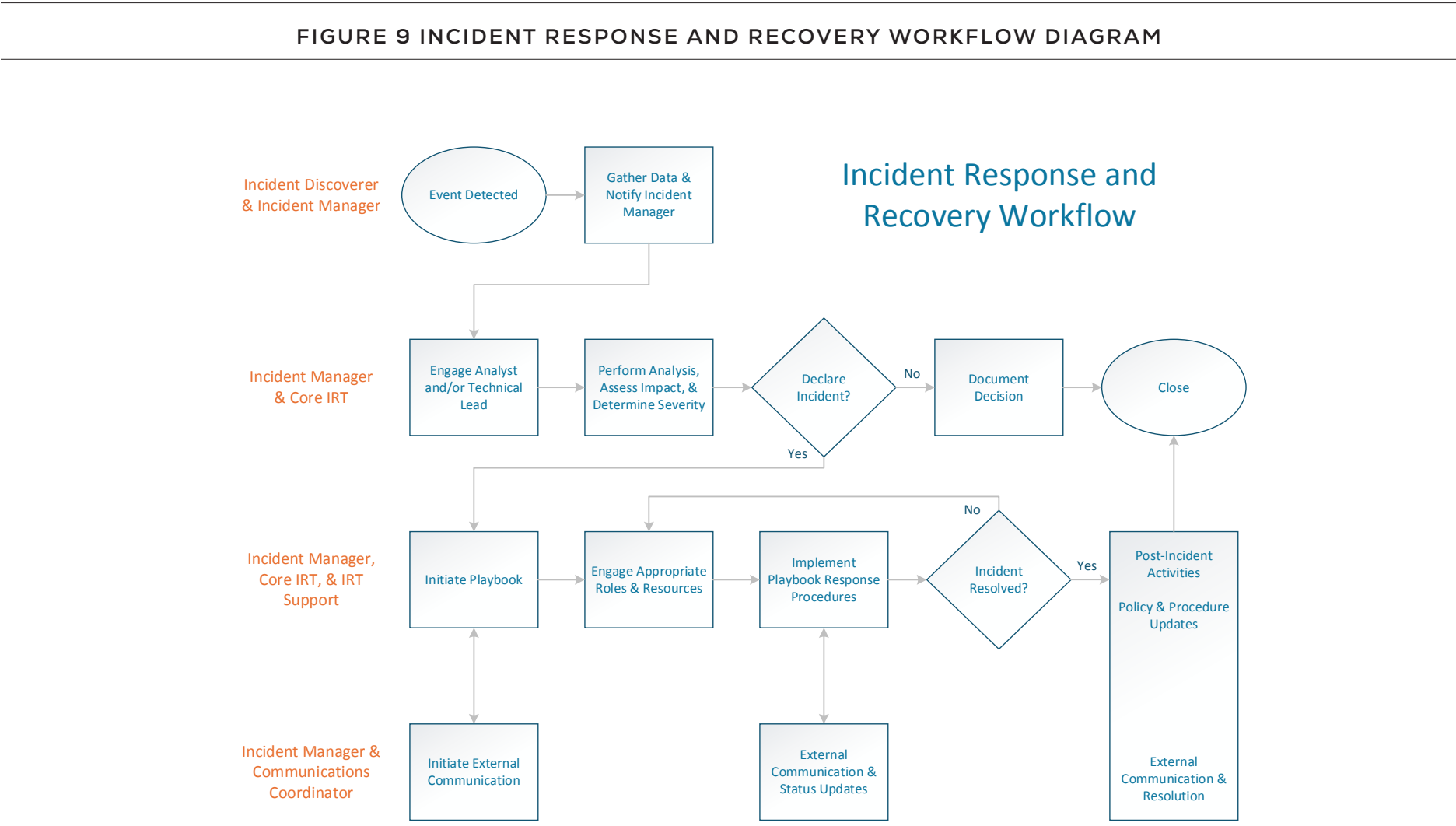
A summary diagram of the incident response and recovery communication pathways is provided below.



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 System Staffing & Training 7.1.4.1 Identified Gaps	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 INFRASTRUCTURE 7.2.1 SCADA Platform, Backups, and Standardization 7.2.1.1 Identified Gaps SCADA Hypervisor Infrastructure at HQ: › Largely comprised of legacy devices outside of supported lifecycles housing	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.

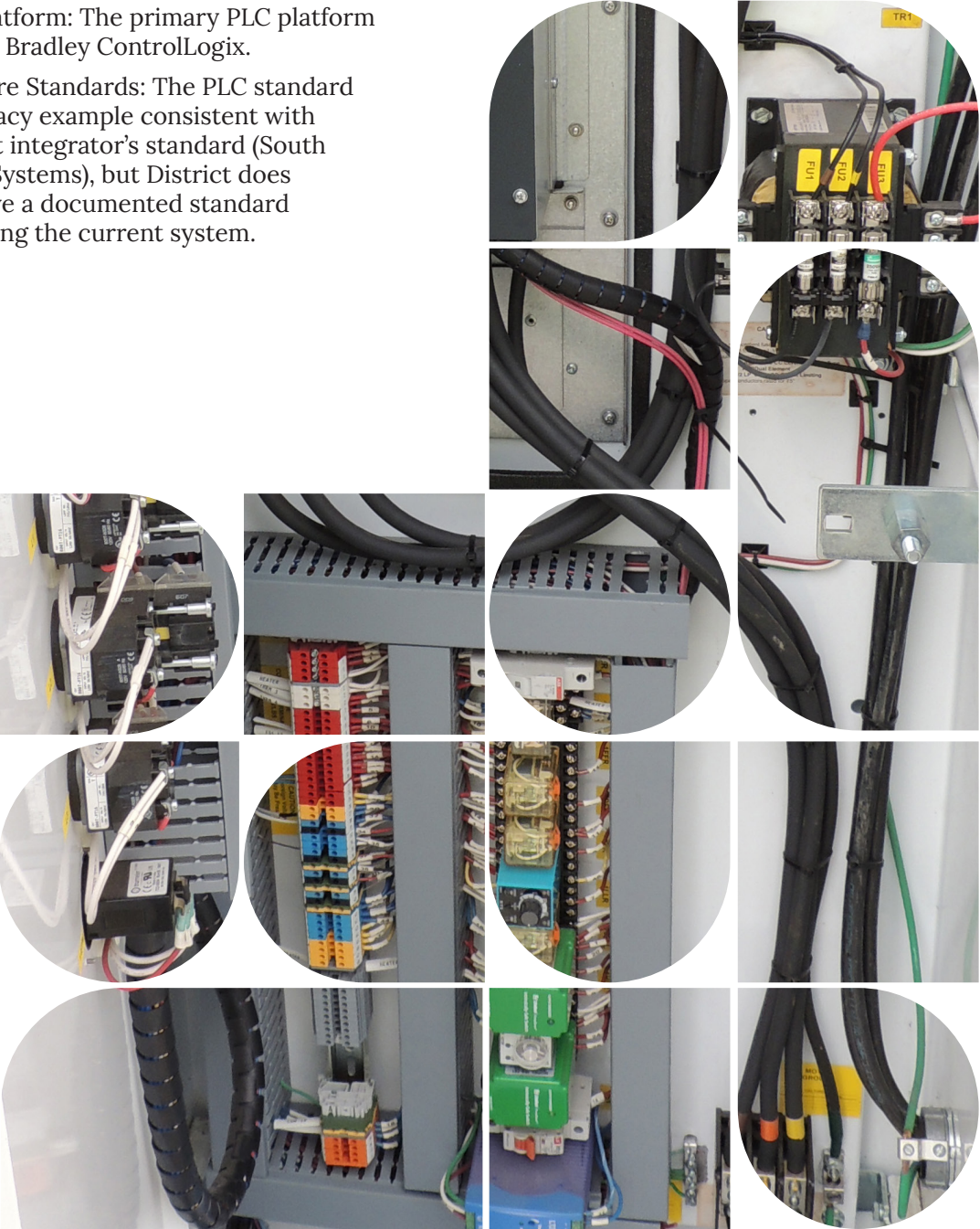
- › PLC Platform: The primary PLC platform is Tesco LIQ's; there are multiple different generations of Tesco PLC's, all of which are legacy models that are proprietary in nature – only Tesco controls services and provides Tesco LIQ PLC's.

- › 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.	8.2.3.4 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.	8.2.3.2 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.	8.2.4 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.	8.2.4.4 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.
		8.2.2.4 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	8.2.3.3 Integration with SCADA Operations › Infrastructure monitoring shall operate independently of SCADA application alarms while supporting integration where beneficial for operational awareness.	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	

8.2.5 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. 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	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. 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	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. 8.4.6 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. 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 CYBERSECURITY STANDARDS 8.5.1 Overview › The District's Cybersecurity Requirements	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. 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	All future SCADA and OT system design, implementation, and integration efforts shall adhere to the CRS and associated District cybersecurity policies. 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
---	--	--

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

