PROFESSIONAL CONSULTANT SERVICES AGREEMENT

OPEN SYSTEMS INTERNATIONAL, INC.

Upgrade of Existing Open System International (OSI) Based Electric Supervisory Control and Data Acquisition (SCADA) System and EMS Systems

THIS PROFESSIONAL CONSULTANT SERVICES AGREEMENT ("Agreement") is made and entered into this_____day of _____ , 2022 ("Effective Date"), by and between the CITY OF RIVERSIDE, a California charter city and municipal corporation ("City"), and OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation ("Consultant").

1. **Scope of Services**. City agrees to retain and does hereby retain Consultant and Consultant agrees to provide the services more particularly described in Exhibit "A," "Scope of Services" ("Services"), attached hereto and incorporated herein by reference, in conjunction with Upgrade of Existing Open System International (OSI) Based Electric Supervisory Control and Data Acquisition (SCADA) System and EMS System ("Project").

2. **Term**. This Agreement shall be effective on the date first written above and shall remain in effect until November 30, 2027, unless otherwise terminated pursuant to the provisions herein.

3. **Compensation/Payment**. Consultant shall perform the Services under this Agreement for the total sum not to exceed Two Million One Hundred Twenty-One Thousand One Hundred Sixteen Dollars ($2,121,116), payable in accordance with the terms set forth in Exhibit "B." Said payment shall be made in accordance with City's usual accounting procedures upon receipt and approval of an itemized invoice setting forth the services performed. The invoices shall be delivered to City at the address set forth in Section 4 hereof.

4. **Notices**. Any notices required to be given, hereunder shall be in writing and shall be personally served or given by mail. Any notice given by mail shall be deemed given when deposited in the United States Mail, certified and postage prepaid, addressed to the party to be served as follows:

To City

Public Utilities Department
City of Riverside
Attn: Jennifer Tavaglione
3435 14th Street
Riverside, CA 92501

To Consultant

Open Systems International, Inc.
Attn: Doug Nelson
4101 Arrowhead Drive
Medina, MN 55340-0649

5. Prevailing Wage. If applicable, Consultant and all subcontractors are required to pay the general prevailing wage rates of per diem wages and overtime and holiday wages determined by the Director of the Department of Industrial Relations under Section 1720 et seq. of the California Labor Code and implemented by Resolution No. 13346 of the City Council of the City of Riverside. The Director's determination is available on-line at www.dir.ca.gov/dlsr/DPreWageDetermination.htm and is referred to and made a part hereof; the wage rates therein ascertained, determined, and specified are referred to and made a part hereof as though fully set forth herein.

6. Contract Administration. A designee of the City will be appointed in writing by the City Manager or Department Director to administer this Agreement on behalf of City and shall be referred to herein as Contract Administrator.

7. Standard of Performance. While performing the Services, Consultant shall exercise the reasonable professional care and skill customarily exercised by reputable members of Consultant's profession practicing in the Metropolitan Southern California Area, and shall use reasonable diligence and best judgment while exercising its professional skill and expertise.

8. Personnel. Consultant shall furnish all personnel necessary to perform the Services and shall be responsible for their performance and compensation. Consultant recognizes that the qualifications and experience of the personnel to be used are vital to professional and timely completion of the Services. The key personnel listed in Exhibit "C" attached hereto and incorporated herein by this reference and assigned to perform portions of the Services shall remain assigned through completion of the Services, unless otherwise mutually agreed by the parties in writing, or caused by hardship or resignation in which case substitutes shall be subject to City approval.

9. Assignment and Subcontracting. Neither party shall assign any right, interest, or obligation in or under this Agreement to any other entity without prior written consent of the other party. In any event, no assignment shall be made unless the assignee expressly assumes the obligations of assignor under this Agreement, in a writing satisfactory to the parties. Consultant acknowledges that any assignment may, at the City's sole discretion, require City Manager and/or City Council approval. Consultant shall not subcontract any portion of the work required by this Agreement without prior written approval by the responsible City Contract Administrator. Subcontracts, if any, shall contain a provision making them subject to all provisions stipulated in this Agreement, including without limitation, the insurance obligations set forth in Section 12. The Consultant acknowledges and agrees that the City is an intended beneficiary of any work performed by any subcontractor for purposes of establishing a duty of care between any subcontractor and the City.

10. Independent Contractor. In the performance of this Agreement, Consultant, and Consultant's employees, subcontractors and agents, shall act in an independent capacity as independent contractors, and not as officers or employees of the City of Riverside. Consultant acknowledges and agrees that the City has no obligation to pay or withhold state or federal taxes or to provide workers' compensation or unemployment insurance to Consultant, or to Consultant's

employees, subcontractors and agents. Consultant, as an independent contractor, shall be responsible for any and all taxes that apply to Consultant as an employer.

11. Indemnification.

11.1 **Design Professional Defined.** For purposes of this Agreement, "Design Professional" includes the following:

A. An individual licensed as an architect pursuant to Chapter 3 (commencing with Section 5500) of Division 3 of the Business and Professions Code, and a business entity offering architectural services in accordance with that chapter.

B. An individual licensed as a landscape architect pursuant to Chapter 3.5 (commencing with Section 5615) of Division 3 of the Business and Professions Code, and a business entity offering landscape architectural services in accordance with that chapter.

C. An individual registered as a professional engineer pursuant to Chapter 7 (commencing with Section 6700) of Division 3 of the Business and Professions Code, and a business entity offering professional engineering services in accordance with that chapter.

D. An individual licensed as a professional land surveyor pursuant to Chapter 15 (commencing with Section 8700) of Division 3 of the Business and Professions Code, and a business entity offering professional land surveying services in accordance with that chapter.

11.2 **Defense Obligation For Design Professional Liability.** Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel acceptable to City. Consultant will reimburse City for reasonable defense costs for claims arising out of Consultant's professional negligence based on the percentage of Consultant's liability. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.3 **Indemnity For Design Professional Liability.** When the law establishes a professional standard of care for Consultant's services, to the fullest extent permitted by law,

Consultant shall indemnify, protect and hold harmless the City and the City's employees, officers, managers, agents, and Council Members ("Indemnified Parties") from and against any and all claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including counsel and expert fees), judgment, civil fines and penalties, liabilities or losses of any kind or nature whatsoever to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party.

11.4 **Defense Obligation For Other Than Design Professional Liability.** Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all third party claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings to the extent caused by: 1) the Services, work, activities, operations, or duties of the Consultant, or of anyone employed by or working under the Consultant, or 2) any breach of the Agreement by the Consultant. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.5 **Indemnity For Other Than Design Professional Liability.** Except as to the negligence or willful misconduct of the City, Consultant agrees to indemnify, protect and hold harmless the Indemnified Parties from and against any third party claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including reasonable counsel and expert fees), judgment, civil fine and penalties, liabilities or losses of any kind or nature whatsoever, to the extent caused by Consultant's performance of the Services, work, activities, operations or duties, or anyone employed by or working under the Consultant or for services rendered to Consultant in the performance of this Agreement by a party directly under Consultant's control and direction, notwithstanding that the City may have benefited from its work or services. This indemnification provision shall apply to any acts, omissions, negligence, recklessness, or willful misconduct, whether active or passive, on the part of the Consultant or anyone employed or working under the Consultant.

12. Insurance.

12.1 **General Provisions.** Prior to the City's execution of this Agreement, Consultant shall provide satisfactory evidence of, and shall thereafter maintain during the term of this Agreement, such insurance policies and coverages in the types, limits, forms and ratings required herein. The rating and required insurance policies and coverages may be modified in writing by the City's Risk Manager or City Attorney, or a designee, unless such modification is prohibited by law. Consultant may provide the types and limits of insurance hereunder by any combination of primary, excess, or self-insurance.

12.1.1 **Limitations.** The limits of coverage in this Section 12 shall not constitute any limitation or cap on Consultant's indemnification obligations under Section 11 hereof.

12.1.2 **Ratings.** Any insurance policy or coverage provided by Consultant or subcontractors as required by this Agreement shall be deemed inadequate and a material breach of this Agreement, unless such policy or coverage is issued by insurance companies authorized to transact insurance business in the State of California with a policy holder's rating of A or higher and a Financial Class of VII or higher.

12.1.3 **Cancellation.** The policies shall not be canceled unless thirty (30) days' prior written notification of intended cancellation has been given to City by certified or registered mail, postage prepaid.

12.1.4 **Adequacy**. The City, its officers, employees and agents make no representation that the types or limits of insurance specified to be carried by Consultant pursuant to this Agreement are adequate to protect Consultant. If Consultant believes that any required insurance coverage is inadequate, Consultant will obtain such additional insurance coverage as Consultant deems adequate, at Consultant's sole expense.

12.2 **Workers' Compensation Insurance.** By executing this Agreement, Consultant certifies that Consultant is aware of and will comply with Section 3700 of the Labor Code of the State of California requiring every employer to be insured against liability for workers' compensation, or to undertake self-insurance before commencing any of the work. Consultant shall carry the insurance or provide for self-insurance required by California law to protect said Consultant from claims under the Workers' Compensation Act. Prior to City's execution of this Agreement, Consultant shall file with City either 1) a certificate of insurance showing that such insurance is in effect, or that Consultant is self-insured for such coverage, or 2) a certified statement that Consultant has no employees, and acknowledging that if Consultant does employ any person, the necessary certificate of insurance will immediately be filed with City. Consultant also agrees to issue a waiver of subrogation in favor of the City of Riverside pertaining to the Consultant's Workers Compensation policy.

12.3 **Commercial General Liability and Automobile Insurance.** Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, commercial general liability insurance and automobile liability insurance as required to insure Consultant against damages for personal injury, including accidental death, as well as from claims for property damage, which may arise from or which may concern operations by anyone directly or indirectly employed by, connected with, or acting for or on behalf of Consultant. The City, and its officers, employees and agents, shall be named as additional insureds under the Consultant's insurance policies.

12.3.1 Consultant's commercial general liability insurance policy shall cover both bodily injury (including death) and property damage (including, but not limited to, premises operations liability, products-completed operations liability, personal injury liability, and liability assumed under an insured contract) in an amount of $1,000,000 per occurrence and a general aggregate limit in the amount of $2,000,000.

12.3.2 Consultant's automobile liability policy shall cover both bodily injury and property damage in an amount of $1,000,000 per occurrence and an aggregate limit of

$1,000,000. All of Consultant's automobile and/or commercial general liability insurance policies shall cover all vehicles used in connection with Consultant's performance of this Agreement, which vehicles shall include, but are not limited to, Consultant non-owned vehicles and hired vehicles.

12.3.3 Prior to City's execution of this Agreement, certificates of insurance along with additional insured endorsements and any applicable self-insurance letters acceptable to the City evidencing the coverage required by this Agreement, for both commercial general and automobile liability insurance, shall be filed with City. Said policies shall be in the usual form of commercial general and automobile liability insurance policies, but shall include the following provisions:

It is agreed that the City of Riverside, and its officers and employees are included as additional insureds under this policy, solely for work done by and on behalf of the named insured for the City of Riverside.

12.3.4 The insurance policy or policies shall also comply with the following provisions:

a. The workers' compensation policy, commercial general liability policy, and automobile liability policy shall be endorsed, to the extent of Consultant's liabilities under this Agreement, to waive any right of subrogation against the City and its sub-consultants, employees and officers for services performed under this Agreement.

b. If the policy is written on a claims made basis, the certificate should so specify and the policy must continue in force for one year after completion of the services. The retroactive date of coverage must also be listed.

c. The commercial general liability policy shall specify that the insurance provided by Consultant, to the extent of Consultant's liabilities under this Agreement, will be considered primary and not contributory to any other insurance available to the City, or its equivalent.

12.4 **Errors and Omissions Insurance.** Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, errors and omissions professional liability insurance in the amount of $1,000,000 to protect the City from claims resulting from the Services.

12.5 **Technology Professional Liability.** Prior to City's execution of this Agreement, Consultant shall provide and maintain during the term of this Agreement technology errors and omissions professional liability insurance with a limit of $2,500,000 per occurrence or claim, $2,500,000 aggregate, to protect the City from claims resulting from the Consultant's

professional services as described specifically herein. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

12.6 **Cyber Liability Insurance.** Prior to City's execution of this Agreement, Consultant shall provide and maintain during the term of this Agreement cyber liability insurance with a limit of $2,500,000 per occurrence or claim, $2,500,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

12.7 **Subcontractors' Insurance.** To the extent applicable to Consultant's Work, Consultant shall require all of its subcontractors to carry insurance in an amount sufficient to cover the risk of injury, damage, or loss that may be caused by the subcontractors' scope of work and activities provided in furtherance of this Agreement, including, but without limitation, the following coverages: Workers Compensation, Commercial General Liability, Errors and Omissions, and Automobile liability. Upon City's request, Consultant shall provide City with satisfactory evidence that Subcontractors have obtained insurance policies and coverages required by this section.

13. Limitation of Liability and Consequential Damages Disclaimer.

13.1 CONSULTANT AND ITS AFFILIATES WILL NOT BE LIABLE FOR DAMAGES CAUSED BY DELAY IN PERFORMANCE. THE REMEDIES OF CITY STATED IN THIS CONTRACT ARE EXCLUSIVE. REGARDLESS OF THE TYPE OF THE CLAIM (WHETHER BASED IN CONTRACT, INFRINGEMENT, NEGLIGENCE, STRICT LIABILITY, OTHER TORT OR OTHERWISE), CONSULTANT'S AND ITS AFFILIATES' LIABILITY TO CITY AND ITS AFFILIATES WILL NEVER EXCEED THE CONTRACT PRICE.

13.2 **NEITHER PARTY WILL EVER BE LIABLE FOR (A) DAMAGES FOR LOSS OR CORRUPTION OF DATA OR CYBER ATTACKS, OR (B) INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES. "CONSEQUENTIAL DAMAGES" INCLUDE BUT ARE NOT LIMITED TO LOSS OF ANTICIPATED PROFITS, REVENUE, PRODUCTION OR USE, AND COSTS INCURRED INCLUDING WITHOUT LIMITATION FOR CAPITAL, FUEL AND POWER, REPLACEMENT PRODUCT, AND CLAIMS OF EACH PARTY'S AFFILIATES.**

14. Business Tax. Consultant understands that the Services performed under this Agreement constitutes doing business in the City of Riverside, and Consultant agrees that Consultant will register for and pay a business tax pursuant to Chapter 5.04 of the Riverside Municipal Code and keep such tax certificate current during the term of this Agreement.

15. Time of Essence. Time is of the essence for each and every provision of this Agreement.

16. City's Right to Employ Other Consultants. City reserves the right to employ other Consultants in connection with the Project. If the City is required to employ another consultant to complete Consultant's work, due to the failure of the Consultant to perform, or due to the breach of any of the provisions of this Agreement, the City reserves the right to seek reimbursement from Consultant.

17. Accounting Records. Consultant shall maintain complete and accurate records with respect to its quoted price under this Agreement. All such records shall be clearly identifiable. Consultant shall allow a representative of City during normal business hours to examine, audit, and make transcripts or copies of such records and any other documents created pursuant to this Agreement. . Consultant shall allow inspection of all work, data, documents, proceedings, and activities related to the Agreement for a period of three (3) years from the date of final payment under this Agreement.

18. Confidentiality. All ideas, memoranda, specifications, plans, procedures, drawings, descriptions, computer program data, input record data, written information, and other materials either created by or provided to Consultant in connection with the performance of this Agreement shall be held confidential by Consultant, except as otherwise directed by City's Contract Administrator. Nothing furnished to Consultant which is otherwise known to the Consultant or is generally known, or has become known, to the related industry shall be deemed confidential. Consultant shall not use City's name or insignia, photographs of the Project, or any publicity pertaining to the Services or the Project in any magazine, trade paper, newspaper, television or radio production, website, or other similar medium without the prior written consent of the City.

19. Ownership of Deliverables.. All reports, maps, drawings and other contract deliverables prepared under this Agreement by Consultant that are specifically identified as being a deliverable under the applicable specifications shall be the property of City, subject to software licensing and other applicable intellectual property provisions of this agreement. Consultant shall not release to others confidential information furnished by City without prior express written approval of City.

20. Copyrights. To the extent any work is specifically and exclusively identified in the applicable mutually agreed specifications as "Custom Work Product" provided for the City, Consultant assigns all right, title and interest in such Custom Work Product to City, and agrees to provide all assistance reasonably requested by City in the establishment of its intellectual property rights in such work, such assistance to be provided at City's expense.

21. Conflict of Interest. Consultant, for itself and on behalf of the individuals listed in Exhibit "C," represents and warrants that by the execution of this Agreement, they have no interest, present or contemplated, in the Project affected by the above-described Services. Consultant further warrants that neither Consultant, nor the individuals listed in Exhibit "C" have any real property, business interests or income interests that will be affected by this project or, alternatively, that Consultant will file with the City an affidavit disclosing any such interest.

22. Solicitation. Consultant warrants that Consultant has not employed or retained any person or agency to solicit or secure this Agreement, nor has it entered into any agreement or understanding for a commission, percentage, brokerage, or contingent fee to be paid to secure this Agreement. For breach of this warranty, City shall have the right to terminate this Agreement without liability and pay Consultant only for the value of work Consultant has actually performed, or, in its sole discretion, to deduct from the Agreement price or otherwise recover from Consultant the full amount of such commission, percentage, brokerage or commission fee. The remedies specified in this section shall be in addition to and not in lieu of those remedies otherwise specified in this Agreement.

23. General Compliance With Laws. Consultant shall keep fully informed of federal, state and local laws and ordinances and regulations which in any manner affect those employed by Consultant, or in any way affect the performance of services by Consultant pursuant to this Agreement. Consultant shall at all times observe and comply with all such laws, ordinances and regulations, and shall be solely responsible for any failure to comply with all applicable laws, ordinances and regulations. Consultant represents and warrants that Consultant has obtained all necessary licenses to perform Scope of Services and that such licenses are in good standing. Consultant further represents and warrants that the services provided herein shall conform to all ordinances, policies and practices of the City of Riverside.

24. Waiver. No action or failure to act by a Party shall constitute a waiver of any right or duty afforded a Party under this Agreement, nor shall any such action or failure to act constitute approval of or acquiescence in any breach thereunder, except as may be specifically, provided in this Agreement or as may be otherwise agreed in writing.

25. Amendments. This Agreement may be modified or amended only by a written agreement and/or change order executed by the Consultant and City

26. Termination. City, by notifying Consultant in writing, shall have the right to terminate any or all of Consultant's services and work covered by this Agreement at any time. In the event of such termination, Consultant may submit Consultant's final written statement of the amount of Consultant's services as of the date of such termination based upon the ratio that the work completed bears to the total work required to make the report complete, subject to the City's rights under Sections 16 and 27 hereof. In ascertaining the work actually rendered through the termination date, City shall consider completed work, work in progress and complete and incomplete reports and other documents only after delivered to City.

26.1 Other than as stated below, City shall give Consultant thirty (30) days' prior written notice prior to termination.

26.2 City may terminate this Agreement upon fifteen (15) days' written notice to Consultant, in the event:

26.2.1 Consultant substantially fails to perform or materially breaches the Agreement; or

26.2.2 City decides to abandon or postpone the Project.

27. Offsets. Consultant acknowledges and agrees that with respect to any business tax or penalties thereon, utility charges, invoiced fee or other debt which Consultant owes or may owe to the City under this Agreement, City reserves the right to withhold and offset said amounts from payments or refunds or reimbursements owed by City to Consultant. Notice of such withholding and offset, shall promptly be given to Consultant by City in writing. In the event of a dispute as to the amount owed or whether such amount is owed to the City, City will hold such disputed amount until either the appropriate appeal process has been completed or until the dispute has been resolved.

28. Successors and Assigns. This Agreement shall be binding upon City and its successors and assigns, and upon Consultant and its permitted successors and assigns, and shall not be assigned by Consultant, either in whole or in part, except as otherwise provided in paragraph 9 of this Agreement.

29. Venue. Any action at law or in equity brought by either of the parties hereto for the purpose of enforcing a right or rights provided for by this Agreement shall be tried in the State and Federal courts in: (1) Minnesota, USA, for any claim brought against Consultant by City; or (2) the local legal jurisdiction of City (e.g., home state, province, country, etc.) for any claim brought against City by Consultant. In the event of multiple claims, the first to file shall control venue as provided above. In the event either party hereto shall bring suit to enforce any term of this Agreement or to recover any damages for and on account of the breach of any term or condition of this Agreement, it is mutually agreed that each party will bear their own attorney's fees and costs.

30. Nondiscrimination. During Consultant's performance of this Agreement, Consultant shall not discriminate on the grounds of race, religious creed, color, national origin, ancestry, age, physical disability, mental disability, medical condition, including the medical condition of Acquired Immune Deficiency Syndrome (AIDS) or any condition related thereto, marital status, sex, genetic information, gender, gender identity, gender expression, or sexual orientation, military and veteran status, in the selection and retention of employees and subcontractors and the procurement of materials and equipment, except as provided in Section 12940 of the California Government Code. Further, Consultant agrees to conform to the requirements of the Americans with Disabilities Act in the performance of this Agreement.

31. Severability. Each provision, term, condition, covenant and/or restriction, in whole and in part, of this Agreement shall be considered severable. In the event any provision, term, condition, covenant and/or restriction, in whole and/or in part, of this Agreement is declared invalid, unconstitutional, or void for any reason, such provision or part thereof shall be severed from this

Agreement and shall not affect any other provision, term, condition, covenant and/or restriction of this Agreement, and the remainder of the Agreement shall continue in full force and effect.

32. Authority. The individuals executing this Agreement and the instruments referenced herein on behalf of Consultant each represent and warrant that they have the legal power, right and actual authority to bind Consultant to the terms and conditions hereof and thereof.

33. Entire Agreement. This Agreement constitutes the final, complete, and exclusive statement of the terms of the agreement between the parties pertaining to the subject matter of this Agreement, and supersedes all prior and contemporaneous understandings or agreements of the parties. Neither party has been induced to enter into this Agreement by and neither party is relying on, any representation or warranty outside those expressly set forth in this Agreement.

34. Interpretation. City and Consultant acknowledge and agree that this Agreement is the product of mutual arms-length negotiations and accordingly, the rule of construction, which provides that the ambiguities in a document shall be construed against the drafter of that document, shall have no application to the interpretation and enforcement of this Agreement.

34.1 Titles and captions are for convenience of reference only and do not define, describe or limit the scope or the intent of the Agreement or any of its terms. Reference to section numbers, are to sections in the Agreement unless expressly stated otherwise.

34.2 This Agreement shall be governed by and construed in accordance with the laws of the State of Minnesota in effect at the time of the execution of this Agreement.

34.3 In the event of a conflict between the body of this Agreement and Exhibit "A" - Scope of Services hereto, the terms contained in Exhibit "A" shall be controlling.

35. Exhibits. The following exhibits attached hereto are incorporated herein to this Agreement by this reference:

Exhibit "A" - Scope of Services
Exhibit "B" - Compensation
Exhibit "C" - Key Personnel
Exhibit "D" – Software Support Plan
Exhibit "E" – Software License Agreement
Exhibit "F" – OSI Cybersecurity Obligations
Exhibit "G" – OSI Patch Management Program

[The rest of this page intentionally left blank. Signatures on Next Page]]

IN WITNESS WHEREOF, City and Consultant have caused this Agreement to be duly executed the day and year first above written.

CITY OF RIVERSIDE, a California charter city and municipal corporation

By: _____
City Manager

Attest: _____
City Clerk

OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation

By: _____

ALBERT ELIASEN
[Printed Name]

PRESIDENT
[Title]

By: _____

SEAN EGAN
[Printed Name]

VP OF FINANCE
[Title]

Certified as to Availability of Funds:

By: _____
for Chief Financial Officer

Approved as to Form:

By: _____
Assistant City Attorney

\\Rc-citylaw\cycom\WPDOCS\D002\P032\00656182.DOCX
20-0632 SDW 06/02/22

Exhibit "A"
Scope of Services

Project Overview

The proposed project consists of an OSI **monarch**™ software upgrade with an infrastructure and hardware migration. This project will be conducted in a single phase, minimizing project risk and delivery time, and providing for the most cost-effective solution to RPU.

The intent of the project is to bring the system up to date to the latest release of the OSI software. The goal is, at a minimum, to retain all functionality present in the current RPU systems, upgraded database systems, and take advantage of the enhancements and standard features available with new releases of the OSI software. RPU will not be the initial install of any new OSI products or modules.

The OSI monarch architecture has a built-in high availability subsystem that controls all synchronization and failover strategy between redundant servers, functions and sites without the need for dependence on 3rd party clustering solutions or other custom hardware high availability solutions. The system utilizes a data replication function to transfer data between the hot and standby systems. The frequency of the data replication is configurable. Under normal operating conditions, the system operates with one set of servers performing real-time online functions (Primary System) with the other set of servers acting as backups (Backup System). In the event of a Primary System failure, the Backup System comes online and performs all assigned critical system functions.

OSI supports all common third-party backup/recovery IT solutions across a wide range of technologies. Although it may have been common to implement a tape-based backup solution, other technologies, such as disk-based, direct-attached storage (DAS), network-attached storage (NAS) and storage area network (SAN) solutions have all been recently implemented and integrated with the OSI system. Third-party backup automation software is commonly used to automate backups at user-defined intervals. Veritas NetBackup, Acronis, Veeam, and Avamar are common OSI user selections for this software. Both the operating system information and OSI system information is typically archived such that the system can be completely and efficiently restored to its original configuration in the event of a disaster."

General responsibilities and an implementation plan are described below. These descriptions include project activities and responsibilities.

This Statement of Work is purposed to complement its associated quotation, which includes additional information such as project milestones.

1. General Scope of Services

1.1 OSI General Responsibilities:

OSI will be responsible for the following implementation services:

1.1.1 **Project Management, Preparation and Planning** – Including preparation planning, OSI will develop a project plan including an overall schedule, will manage OSI resources to ensure timelines and dates are met, provide overall leadership for OSI Upgrade activities. This may include defining project schedules, communication plans, identifying and creating risk lists, management of issues, and status reporting.

1.1.2 **Design -** OSI engineers will hold internal design, planning and review meetings prior to onsite implementation. Design discussions shall include RPU. RPU will approve all design decisions prior to project execution. OSI will develop and document a design to include physical and logical design of system, system specifications, migration strategy and design, and configuration of all services and features. OSI will be responsible for conversion and testing of RPU's existing databases and displays, operator notes, user settings, etc. to the most recent, certified monarch format.

1.1.3 **Testing -** OSI will create test plans/documentation, submit them to RPU for approval, and conduct testing in accordance to mutually agreed upon procedures. OSI will test all applications during factory testing at OSI's facility. A formal SAT will be performed at RPU's facility. Up to 5 days of dedicated testing will be performed with additional testing provided on a time and materials basis (not to exceed 10 days). Any delays causing extension of site acceptance testing and any associated costs will be reviewed and agreed upon by both parties. Testing plan will be determined and agreed upon as part of the kickoff activities. Reference Appendix A for Performance & Response Requirements.

1.1.4 **Deployment -** OSI will travel to site to perform system installation, configuration and testing.

1.1.5 **Training** - OSI will provide onsite Electric Operations SCADA operator training (onsite at RPU's facility). This will be conducted in a hands-on fashion by the project engineer assigned to perform the software installation. Separately, **OSI University** training will be provided for the new Forecast and SOM Planner products. Custom onsite admin training in an OSI University format will also be provided. Training plan will be determined and agreed upon as part of project kickoff activities.

1.1.6 **Knowledge Transfer** – OSI will provide RPU system administration staff with the knowledge required to maintain and troubleshoot the system deployment. This knowledge transfer will provide RPU with ability to manage and maintain the system on a "go forward" basis.

1.1.7 **Cutover** - Project team will assist with cutover plan in the event that there are issues with cutover to the new system. Since the systems will be running in parallel the plan would be to fail back if needed. See section 2.1.

1.1.7.1 OSI will provide a cutover plan to be approved by RPU. OSI will assist with cutover. OSI will provide post Implementation Support and Documentation.

1.2 RPU Responsibilities:

RPU acknowledges that its timely provision to OSI of facilities, equipment, assistance, cooperation, documents, reviews, complete and accurate information and data from RPU officers,

agents, and employees, and suitably configured computer products (collectively, "cooperation") is essential to the performance of any Services set forth in this SOW. RPU acknowledges that OSI's ability to perform the Services and any financial estimate or schedule or milestone commitments related thereto depends upon RPU's cooperation on a timely basis, the additional project scope specifications stated in the section below and RPU fulfillment of the following obligations.

The following are responsibilities and other obligations of the RPU team:

1.2.1 RPU will ensure existing GPS antenna can be reused or will handle procurement and installation of a new antenna, if necessary.

1.2.2 RPU will be responsible for modifying the monarch display for Time Deviation (i.e. deleting null values). It is recommended RPU uses the web user interface that comes with the GPS clocks.

1.2.3 RPU will participate in a 2-Day Data Engineering Workshop in which OSI will train RPU on the OSI Maintenance Server product. It is preferred that RPU travel to OSI for the Data Engineering Workshop. However, if RPU is not able to travel to OSI, the project plan can be reworked to accommodate for a remote Data Engineering Workshop.

1.2.4 RPU will provide all third-party hardware, software licensing and configuration not specifically mentioned in the associated quote.

1.2.5 If required, quote assumes RPU will handle any custom display and database work and will test and verify all external links and interfaces. Displays and databases are considered custom when more than minor adjustments are needed after the displays and databases have been converted over to the new version of monarch.

1.2.6 RPU will be responsible for all work pertaining to the Palo Alto firewalls (i.e. procurement, installation, configuration, etc.). If RPU wants these firewalls included during testing events at OSI's facility, RPU will be responsible for sending them to OSI with an open configuration and credentials for OSI to access them. OSI will provide basic firewall, server, workstation, switches, terminal servers ports and services, etc. configuration guidelines for RPU to use as a reference.

1.2.7 OSI's scope of work pertaining to SCCM is limited to only VM creation. RPU will be responsible for all other necessary procurement, installation, configuration, testing, etc

1.2.8 RPU will provide high-speed (100+Mbps) remote access to server and console hardware if needed (VPN, Remote Desktop Connection, etc.). Dial-up modem connections are insufficient. Latency must be 100ms or less.

1.2.9 RPU will provide sufficient cabinet space and cabling for new hardware. If RPU is not able to provide this, additional cabinets and/or cables can be quoted separately.

1.2.10 Any hardware purchased by RPU will be compliant with monarch™.NET minimum requirements as indicated in the associated quotation.

1.2.11 OSI's scope of work for the smart card evaluation is limited to smart card evaluation effort only. RPU will be responsible for all other procurement, installation, configuration, testing etc. RPU will also be responsible for procuring keyboards with smart card support for the workstations in the associated quote. The workstations in the associated quote do not include keyboards. The laptops in the associated quote have a smart card slot included.

1.2.12 RPU will be responsible for spinning up new VMs and installing and configuring all third-party software (including OS). OSI will perform a remote OS inspection. Any issues found specific to hardware or OS configuration during the inspection will need to be resolved by RPU. RPU will then be responsible for sending all monarch VM's to OSI's facility via hard drives for monarch installation, configuration and testing.

1.2.13 RPU will be responsible for all installation and configuration for 3rd party VMs (i.e. Active Directory, SCCM, backup/restore, antivirus, etc.). It is assumed these will not be sent to OSI's facility. OSI will provide specific settings require by the software in Active Directory, group policy, etc. so that RPU can configure the VMs correctly.

1.2.14 Quote assumes RPU will send OSI at least two (2) workstations for testing activities at OSI's facility.

1.2.15 RPU will be responsible for all required network switch and firewall configuration.

1.3 Additional Project Scope Specifications

1.3.1 OSI acknowledges that its timely notification to RPU in the event office accommodations, facilities, equipment, assistance, cooperation, complete and accurate information and data from RPU officers, agents, and employees, and suitably configured computer products (collectively, "cooperation") are not adequate, is essential to the performance of any Services set forth in this SOW.

1.3.2 OSI will not be responsible for RPU delays, and the consequent costs incurred.

1.3.3 RPU will not be responsible for OSI delays, and the consequent costs incurred.

1.3.4 The Services and resulting Deliverables may include advice and recommendations, but RPU agrees that all decisions in connection with the implementation of such advice and recommendations will be the responsibility of, and made by, RPU.

1.3.5 Outside of items shown in the associated quotation, OSI is not providing any third-party software, tools or equipment or materials to RPU.

1.3.6 RPU is responsible to negotiate warranties for any third-party software or other products it licenses or acquires.

1.3.7 OSI may rely upon any standard operating procedures or practices of RPU and any direction or regulatory or other guidance provided by RPU.

1.3.8 RPU is responsible for the identification and interpretation of, and ensuring compliance with, any laws, statutes, rules, regulations and standards applicable to its or its affiliates' business or operations.

1.3.9 OSI is not providing any warranty regarding, and is not liable for, any third party or RPU software, documentation, equipment, tools or other products or materials (even if recommended by OSI).

1.4 Mutual Responsibilities

In support of the Services provided hereunder, both OSI and RPU shall:

1.1.4 Assign a primary contact and point of authorization as the project manager. The single points of contact will be responsible for facilitating all communications between both parties and for issue resolution, activity scheduling, interview scheduling, and information collection and dissemination. The timeliness of communications and other activities will directly affect both parties' ability to meet agreed upon schedule deadlines.

1.1.5 Be responsible for the performance of its employees and agents, including any contribution they make to the Services (including Deliverables), and for the accuracy and completeness of all data, information and materials provided. Performance is dependent upon timely decisions and approvals in connection with the Services and OSI and RPU are entitled to rely on all decisions and approvals of one another.

1.1.6 Acknowledge that its failure or delay to cooperate or furnish items as contemplated under this SOW or in performing its other responsibilities or obligations under this SOW, or a delay caused by any third-party vendor providing services or products that impact the Services, will be considered responsibility of the party impacting the Services and an excusable delay or failure of the impacted party to the extent the Services are impeded or delayed.

1.1.7 Have resources assigned to the project which must possess knowledge of existing OSI and RPU processes and have the ability and authority to champion those respective business process changes.

1.1.8 Ensure that the appropriate staff members attend and participate in the required interviews and reviews and are able to discuss the topics presented.

1.1.9 Conduct project review meetings at a mutually agreed upon time and location to discuss the project status, issues, new requirements and overall project satisfaction.

1.1.10 Support and provide representation at these meetings, which will cover performance status update, schedule update, pending changes, open issues and action items.

1.1.11 Support project issue and tracking resolution, by using the Issue Resolution Form to track and review issues.

1.1.12 Coordinate any change to this SOW (whether cost impacting or not) with RPU Project Sponsor and process them using the Change Request Process.

1.1.13 Collaborate to adjust project schedules and re-deploy resources in an expeditious manner in the event of schedule delays that are beyond the control of either party.

1.1.14 Meet at the conclusion of this project to bring to closure the project and capture, discuss and resolve any project issues that may have arisen.

1.1.15 Keep their respective project managers apprised of business, organizational and technical issues that may have an impact on the performance and delivery of this project.

2. System Upgrade Implementation

This section describes the proposed, high-level implementation plan and scope of services for all required system functionality. The required on-site and off-site engineering and implementation services proposed are also described. This project will be approached with a high level of quality control, planning, and testing.

A more detailed implementation plan will be created during the project, which will better define lower-level tasks and associated durations and dates.

2.1 Hardware/Software Upgrade Task List

2.1.1 Hold upgrade kick-off meeting to determine upgrade approach

2.1.2 Hardware/IT review of RPU infrastructure transition

2.1.3 Order new hardware

- OSI-procured hardware (see associated quote for additional details):
  - VM host servers
  - Network attached storage devices
  - Tape drives
  - Workstations and monitors

- Laptops
- KVM switch and associated keyboard, monitor and mouse
- GPS clocks
- Network switches
- OSI Terminus (terminal servers)
- LAN Cabling and Connectors

- RPU-procured hardware:
  - All other hardware not specifically mentioned in the associated quote

2.1.4 Order new third-party software licensing

- OSI-procured third-party software licensing (see associated quote for additional details):
  - MS Visual Studio Professional 2022
    - Used for compiling monarch software
  - Windows Server 2022 OS
    - Server license and device CAL license
    - Downgrade if needed
  - Hyper-V hypervisor
    - Included with Windows Server 2022 licensing
  - Windows 11 Pro OS
    - To be combined with Windows 10 2021 Enterprise LTSC Upgrade license
    - Downgrade if needed
  - Windows 10 2021 Enterprise LTSC Upgrade license
    - To be combined with Windows 11 Pro license
  - Acronis backup/restore
- McAfee Complete Endpoint Protection antivirus
- RPU-procured third-party software licensing:
  - All other third-party software licensing not specifically mentioned in the associated quote

2.1.5 Complete software matrix for OSI and third-party software\

2.1.6 Request and complete as-built list of deliverables as applicable

2.1.7 Determine existing deviations and outstanding support issues

2.1.8 Collect existing system data:

- Real-time database dumps, schemas and sizing information
- rc files
- Calcs
- Custom displays
- Host files
- Shell or batch files
- OpenHIS table schemas (including custom tables)
- License initializer strings

2.1.9 Create IT Plan, User Configuration, IP Hostnames, Open Ports. OSI will provide basic firewall, server, workstation, switches, terminal servers ports and services, etc. configuration guidelines for RPU to use as a reference.

2.1.10 Determine and document product upgrade plans. This includes the following:
- Real-time database conversion plans
- Merge rc file
- List customized OSI displays to be updated
- RDBMS data conversions
  - Includes conversion and historical data backfill (up to five-year's worth) from MSSQL to PostgreSQL
- Any new configuration files or settings
- PI Interface to HSH PI Interface Conversion
- OpenSTLF to Forecast Conversion
- OpenSOM to SOM Planner Conversion
- Compile Calcs

2.1.11 RPU SCADA Implementation
- Receive and install new equipment/infrastructure
- Perform Operating System install and configuration

2.1.12 Determine and document system upgrade plan. Include:
- Review existing deviations
- Script changes, especially osi_autostart and osi_shutdown
- Cutover plan
- Configuration freeze date(s)

2.1.13 OSI products implementation/decommissioning
- Install and configure required products
  - Includes new Maintenance Server and Maintenance GUI products
- Perform applicable conversions and database implementation
- Decommission CHRONUS

2.1.14 Evaluate smart card technology to ensure monarch compatibility and document results

2.1.15 Early delivery of PDS Server(s) for initial testing and conversion activities (if applicable)

2.1.16 Perform Maintenance Server Data Engineering Workshop with RPU

2.1.17 Factory QA testing preparation and execution (no RPU presence required)

2.1.18 Record variances, issue resolution

2.1.19 Testing cleanup, packing and shipping

2.1.20 Site arrival and site integration testing preparation; RPU to assist with interfacing of external systems

2.1.21 Site Acceptance Testing (SAT)

2.1.22 Pre-SAT Testing setup & documentation preparation
- Conduct Pre-SAT Testing activities
- Prepare and submit to RPU SAT testing documentation
- Conduct 1-Week Site Acceptance Testing with OSI at RPU's facility (additional testing billed on a time and materials basis if needed; not to exceed 10 days total)

2.1.23 Run in monitoring mode. OSI to set up before SAT. Run in monitor mode during SAT until cutover.

2.1.24 Record variances, issue resolution

2.1.25 Site testing clean up and commissioning preparation

2.1.26 Conduct onsite operator training on upgraded features

2.1.27 Conduct formal onsite System Administrator training
2.1.28 Perform system cutover
- A cutover plan will be discussed in depth during kickoff. RPU to have input and approve approach. See section above "Determine and Document System Upgrade Plan"

2.1.29 Complete customer support documentation related to any code, configuration, or information specific to the Riverside project for knowledge transfer purposes to maintain on-going system operations from OSI project team to OSI support and the Riverside SCADA team
2.1.30 Transition to customer support

3. Project Deliverables and Acceptance Criteria

Deliverable Name	Description	Occurrence	Acceptance Criteria
Project, design and product documentation	Per the descriptions above, OSI will furnish design documentation including a detailed project plan, project schedule and product documentation designs.	Initial version and updates throughout the project	RPU will approve documentation prior to acceptance (with exception of standard product documentation)
SAT planning documentation	Deliver and review SAT onsite testing) procedures with RPU	Upon completion of design/prep tasks	RPU will approve test planning documentation prior to acceptance
SAT results documentation	Test Case Results documentation indicating successful test results, failed test cases, variance details	Upon completion of testing performed by OSI	RPU will approve all testing documentation prior to acceptance, indicating successful testing completion without any critical or high severity variances
Hardware and 3rd party software	Servers, workstations, OS licenses, etc. as identified in the associated quote.	Upon early PDS delivery and production deployment	N/A – 3rd party equipment will be shipped to RPU in accordance with the accepted project schedule (part of the project documentation)
Upgraded OSI Software Releases	Cutover to upgraded system with new hardware and software	Upon early PDS delivery and production deployment	N/A – Upgraded releases will be shipped to RPU in accordance with the accepted project schedule (part of the project documentation)
Knowledge transfer of upgraded system	Provide training in a hands-on fashion of new and upgraded features	Upon completion of training	Upon completion of all training events

	Provide administration staff with the knowledge required to maintain and troubleshoot the upgraded system		
Technical support	Technical support will be transferred from the old RPU system to the upgraded RPU system. Support will follow the standard support plan currently purchased by RPU.	Upon completion of cutover	Upon completion of project and transition to support

4. Change Management

To ensure the success of this engagement, it is critical that RPU and OSI have a clear understanding of project expectations. The parties will utilize the approach outlined below for managing the scope of the project.

RPU or OSI may propose changes to the Services under this SOW, including Deliverables, scope or any other aspect of the engagement. Changes may be appropriate based upon actual experience or as RPU better understands or redefines its requirements. In addition, changes may be necessary if either RPU or OSI do not comply with any of its responsibilities or other obligations under this SOW or in the event of any deviation from any assumption, constraint, dependency or project scope specification contained in this SOW. The change management process for this engagement consists of the following:

- **Change Initiation** – All proposed changes will be forwarded to, or originated by, the OSI project manager and documented. A copy of the proposed change request will be forwarded to the RPU project manager.
- **Change Validation** – Only when the change request is clearly understood can the project team evaluate the impact of the change and determine whether the change can be accommodated. Therefore, the proposed change will be examined and discussed with the RPU contact identified in this SOW.
- **Change Analysis and Impact Analysis** – OSI will prepare a change analysis and impact analysis using the Change Request form. The impact analysis includes a cost and schedule impact to the engagement, if applicable. This will be reviewed with RPU for approval.
- **Change Implementation** – If approved, the change will be noted as "Approved" and will be incorporated into the schedule and managed for progress. If the change is not approved, the change will be noted as "Rejected" and OSI will continue to perform without regard to the proposed change (to the extent practically possible).

Possible outcomes of a change request, as may be documented in the change analysis and/or impact analysis, include the following:

- Can be accommodated within project resources and timelines;
- Can be accommodated but will require an extension of the schedule;
- Can be accommodated within the current schedule, but additional resources or budget will be required;
- Can be accommodated but additional resources or budget and an extension of the schedule will be required;
- Cannot be accommodated without a significant change to the project or it is not technically, economically or otherwise feasible.
- OSI has no obligation with respect to any change requested by RPU until an appropriate written change order or other amendment to this SOW is approved and signed by RPU and OSI.

5. Issue Resolution Process

All issues for this engagement will be tracked by OSI utilizing the following process:

- Either party may raise an issue
- All issues will be communicated to and tracked by both the RPU SCADA and OSI project managers
- The issues will be electronically tracked in an Issues Log

6. Testing Acceptance Criteria

RPU and OSI agree to the following acceptance criteria for each of the testing phases:

- All planned tests have been executed
- Level of requirement coverage (as per RPU contract) has been met
- No Critical or High Severity defects
- No Medium severity defects left outstanding without a mutually agreed RPU SCADA and OSI work plan
- Product Owner signoff that all of the above steps have been verified.

A variance shall be reported each time a deviation from SOW requirements is detected or a problem in the functionality of the system is encountered during any of the System Tests.

The variance reported shall include a complete description of the variance, including the reference to this SOW and the test procedure being carried out along with an explanation of the expected results and a description of the test conditions/data at the time the variance was detected.

OSI shall document the corrective actions taken to eliminate each variance by providing sufficient detail for the RPU representative to determine the necessity for and extent of the re-testing of the offending function. This shall include an evaluation of any interaction with previously tested functions, and of any documentation that may require updating as a result of the corrective action. A resolution plan for all outstanding issues will be developed and mutually agreed upon.

The variance report shall be completed when OSI and RPU representatives acknowledge correction of the variance with signatures. The variance reports shall be available to RPU at all times and shall be submitted by OSI to RPU at the conclusion of each test.

OSI will manage and maintain variances electronically via Jira. OSI and RPU will hold regular discussions on variance progress and resolution.

Variance shall be defined as follows as determined by RPU:

1. **Critical** - System Down.
    - These variances are deemed critical as the system is down.
2. **High** - Operational function broken/missing with no workaround.
    - This indicates that a key function required for day-to-day operations is broken or missing and no workaround is available.
3. **Medium** - Operational function broken/missing with a workaround.
    - This indicates that a key function required for day-to-day operations is broken or missing but a workaround is available.

4. **Low** - Minor Defect.
    - A defect with no operational impact and only a minor effect on project progress.
    - A feature with limited or no impact on the operation of the system is broken or missing and no workaround is available.
    - A feature with limited or no impact on operations of the system is broken or missing but a workaround is available.
5. **Enhancement** - Request or Suggestion.
    - These variances indicate a requested enhancement to a product or a general suggestion

6. Other Requirements

Badges will be provided and are required for any RPU SCADA personnel entering OSI's facility. OSI employees will need to be escorted by RPU SCADA personnel while onsite at any RPU facility. In addition, RPU SCADA personnel will be escorted by OSI employees while at OSI's facility.

Potential restrictions due to COVID-19 will be discussed during early phases of the project.

7. Period of Performance

7.1 Term of the SOW

This SOW shall commence within 6 Months of contract acceptance and shall continue without interruption for the duration of the project schedule. A SOW may be terminated in accordance with the termination sections of the Master Contract or as otherwise agreed between the parties. SOWs or renewal SOWs entered into prior to the expiration or other termination of the Master Services Agreement may be completed under the Master Service Agreement terms and conditions in effect when the SOW or renewal SOW was entered into. In no event shall the term of any SOW extend beyond the term of the Master Services Agreement.

7.2 Term of the Project

This project will take place during a 13-month period from start of project (i.e. project kick-off) to conclusion (i.e. commissioning).

7.3. Estimated Schedule/Milestones

SOW effective date	November 2022
Kickoff, Hardware and Software Ordering	June 2023
PDS Staged and Ready for Testing at RPU's location	October 2023
Completion of Factory Q/A Testing	January 2024
QAS and Production System Staged and Ready for Testing at RPU's location	March 2024
Completion of Site Testing	May 2024
Production Cutover	July 2024

Appendix A: Performance & Response Requirements

Performance Test Scenarios	Steady State	High Activity
Test Period	15 minutes	15 minutes
No. of Analogs Changing every scan	20% of all	50% of all
No. of Status Points Changing every scan	20% of all	50% of all
No. of ICCP Analogs (imports per 10 sec.)	500	1000
No. of ICCP Status (imports per 10 sec.)	500	1000
No. of ICCP Analogs (exports per 10 sec.)	500	1000
No. of ICCP Status (exports per 10 sec.)	500	1000
No. of alarms generated per second	50	1000
Periodicity of display requests from five consoles	15 second	10 second
Control Request from at least 3 consoles	2 per minute	10 per minute
Historical Archival of Analogs	1000 points per 5 minute	2000 points per 5 minute
Response Requirements	**Steady State**	**High Activity**
Display Call-up time---------One-lines	1.5 sec.	2 sec.
Display Call-up time---------SCADA Tabulars	1.5 sec.	2 sec.
Display Call-up time---------Alarming Tabulars	2 sec.	2.5 sec.
Control Completion time (local RTU)	1 sec.	1.5 sec.
Alarm Acknowledgment time	1 sec.	1.5 sec.
Alarm Delete time	1 sec.	1.5 sec.

Appendix B: SCADA System Software Sizing

Parameter	Value
Channels	200
Control Points	6000
ICCP Export Points	2000
ICCP Import Points	2000
ICCP VCC Links	8
RTUs	200
Telemetered Points	30500
PI/eDNA Archived Points	100000
Concurrent Lite Client Users	20
OpenView Full Clients	41
Accumulators	500
Analogs	29000
Setpoints	4
Status	22000
Total SCADA Points	51504
ODBC Concurrent Connections	29

Exhibit "B"
Compensation

QUOTATION

Quote Number: 30022
Reference: RPU2021-Q02-B-Rev5

Date: 5/16/2022
Valid Until: 8/1/2022

Quote To:
Riverside Public Utilties
2911 Adams Street
Riverside CA 92504
USA

Attention:
Robert Lovas
(951) 351-6209
rlovas@riversideca.gov

OSI Sales Contact:
Name: Shawn Niebler
Phone: 763-746-7395
Email: Shawn.Niebler@osii.com

Quote Description:
System Upgrade (Staged at RPU)

Description	Qty	Unit Cost	Unit	Extended Cost
Base Quote: System Upgrade (Staged at RPU)				
OSI Hardware				
Terminus - with Dual AC Power Supplies, 32-Ports	2	4,500.00	EA	US$ 9,000.00
OSI Hardware Subtotal:				**US$ 9,000.00**
Third Party Hardware				
VM Host Server - Type 1 Hosting: - (1) SCADA/ICCP VM - (1) FEP VM - (1) HIS VM - (1) APP VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	3	23,880.00	EA	US$ 71,640.00
VM Host Server - Type 2 Hosting: - (1) SCADA/ICCP VM - (1) FEP VM - (1) HIS VM - (1) APP VM - (1) Active Directory VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00

Description	Qty	Unit Cost	Unit	Extended Cost
VM Host Server - Type 3 Hosting: - (1) PI Interface VM - (1) HIS VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00
VM Host Server - Type 4 Hosting: - (1) PI Interface VM - (1) HIS VM - (1) Active Directory VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00
VM Host Server - Type 5 Hosting: - (1) PDS VM - (1) DTS VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00
VM Host Server - Type 6 Hosting: - (1) Security VM - (1) Active Directory VM - (1) Antivirus VM - (1) Storage/SCCM VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00
VM Host Server - Type 7 Hosting: - (1) SCCM VM - (1) Active Directory VM HP Proliant DL380 Gen 10 2.5" Chassis with up to 8 Drives (2) Intel® Xeon® Gold 6242R 3.1GHz, 20C/40T 288GB (2x16+4x64GB) RDIMM RAM 7.2TB (6x2.4TB RAID 10) 10K RPM SAS Disk (4) 1-Gigabit Ethernet Ports Redundant Power Supply 3-Year Foundation Care NBD	1	23,880.00	EA	US$ 23,880.00

Open Systems International Inc.
4101 Arrowhead Drive, Medina MN 55340-9649
Phone: (763) 551-0559 Fax: (763) 404-4007
email: info@osii.com https://www.osii.com

Description	Qty	Unit Cost	Unit	Extended Cost
Workstation -Type 1 HP Z4 G4 Workstation Intel Xeon W-2123 3.6GHz Quad-Core HT 500GB 7.2K RPM SATA Hard Disk 32GB RAM DVD-RW Integrated GbE NIC Additional GbE NIC AMD Radeon Pro W5500 Scroll Mouse 3-Year Basic Hardware, 5x10 NBD Warranty	22	2,220.00	EA	US$ 48,840.00
Monitor HP EliteDisplay E23 G4	42	264.00	EA	US$ 11,088.00
Display HP Z43 42.5-inch 4K UHD	2	888.00	EA	US$ 1,776.00
Workstation - Type 2 Dell Precision 7760 Intel® Xeon® W-11855M 3.2GHz, 6-Core (12 Threads) Processor 32GB (4x8GB) RAM 512GB SSD NVIDIA® RTX™ A4000 Graphics Card Smart Card Slot 3-Year Basic Onsite Service Warranty	15	4,500.00	EA	US$ 67,500.00
HP 18.5" LCD Monitor, Keyboard and Mouse Belkin Standard Power Cord - 120V AC, 15ft	4	1,134.00	EA	US$ 4,536.00
KVM Switch Raritan Dominion KX III KVM-Over-IP 8-Port KVM Switch KVM Cables Belkin Standard Power Cord - 120V AC, 15ft	6	4,620.00	EA	US$ 27,720.00
HPE StoreEasy 1660 NAS 20TB (3x10TB RAID 5 Plus 1xHot Spare) 7.2K RPM SAS Disk	3	12,480.00	EA	US$ 37,440.00
HPE LTO 5 Ultrium 3000 Tape Drive (20) Pack of LTO-5 Tapes	3	4,560.00	EA	US$ 13,680.00
Arbiter 1205C GNSS Synchronized Clock	3	5,160.00	EA	US$ 15,480.00
Cisco Catalyst 48-Port Network Switch (C9200L-48T-4G-E) 3-Year Cisco DNA Essentials 3-Year 8x5 NBD SMARTnet Support	13	4,200.00	EA	US$ 54,600.00
LAN Cabling/Connectors	1	3,720.00	LOT	US$ 3,720.00
Customer Furnished Third Party Hardware All Other Third Party Hardware (i.e. Workstation Keyboards, Firewalls, etc.)	1	0.00	LOT	US$ 0.00
Customer Furnished Smart Cards	1	0.00	LOT	US$ 0.00
Third Party Hardware Subtotal:				**US$ 501,300.00**
OSI Software				
monarch Software Upgrade License Free-of-Charge with Gold Support	1	0.00	EA	US$ 0.00
PI Interface to HSH PI Conversion License Free-of-Charge	1	0.00	EA	US$ 0.00
OpenSTLF to Forecast Conversion License Free-of-Charge	1	0.00	EA	US$ 0.00
OpenSOM to SOM Planner Conversion License Free-of-Charge	1	0.00	EA	US$ 0.00

Description	Qty	Unit Cost	Unit	Extended Cost
OpenHIS Conversion License From MSSQL 2008R2 to PostgreSQL Free-of-Charge	1	0.00	EA	US$ 0.00
Maintenance Server (Centralized DB Editing Subsystem) License Includes DataExplorer and Maintenance Center Standard - Job Deployment Management - Web Platform Product Configuration Management - Configurable Workflow/Approval Processes - Unified Audit Trail - System Explorer Display Versioning Support - Job Deployment Against Study/Offline Instance Free-of-Charge	1	0.00	EA	US$ 0.00
Maintenance GUI (DB/Display Editing User Interface) License Includes Access to DataExplorer, Design Studio, Tabular Builder, OpenODBC, and Tweak Free-of-Charge	6	0.00	EA	US$ 0.00
OpenView GUI Client License (2-Monitor)	6	2,750.00	EA	US$ 16,500.00
OpenView GUI Client License (1-Monitor)	2	2,500.00	EA	US$ 5,000.00
OSI Software Subtotal:				**US$ 21,500.00**
Third Party Software				
Microsoft Visual Studio Professional 2022 Single OLP License Downgrade if Needed	5	516.00	EA	US$ 2,580.00
Acronis Backup 12.5 Advanced Virtual Host License Includes AAP ESD	9	2,052.00	EA	US$ 18,468.00
Acronis Backup 12.5 Advanced Workstation License Includes AAP ESD	37	126.00	EA	US$ 4,662.00
Customer Furnished Third Party Software All Other Third Party Software	1	0.00	LOT	US$ 0.00
Windows Server 2022 Datacenter OLP - 16 Core License Includes Hyper-V Downgrade if Needed	21	6,360.00	EA	US$ 133,560.00
Windows Server 2022 Datacenter OLP - 2 Core License Includes Hyper-V Downgrade if Needed	36	798.00	EA	US$ 28,728.00
Windows Server 2022 Standard OLP - Device CAL Downgrade if Needed	37	42.00	EA	US$ 1,554.00
Windows 11 Professional 64-bit - License Downgrade if Needed	37	168.00	EA	US$ 6,216.00
Microsoft Windows 10 2021 Enterprise LTSC - Upgrade License	37	306.00	EA	US$ 11,322.00
McAfee Complete Endpoint Protection - 1-Year Gold Software Support	67	115.00	EA	US$ 7,705.00
Third Party Software Subtotal:				**US$ 214,795.00**

Open Systems International Inc.
4101 Arrowhead Drive, Medina MN 55340-9649
Phone: (763) 551-0559 Fax: (763) 404-4007
email: info@osii.com https://www.osii.com

Description	Qty	Unit Cost	Unit	Extended Cost
Project Implementation				
System Upgrade Implementation At OSI: - Project Management and Coordination - Project Engineering and Design - NERC CIP Baseline Documentation of System Ports, Users, and Services Necessary for Upgraded System Operation - Remote OS Inspection - VM Import - Cyber Security Evaluation of Network Modifications Required for Upgrade - Configuration and Restriction of Access Control Policies for Applicable Firewall Equipment - Software Installation and Configuration - Database and Display Conversion and Integration - Maintenance Server Data Engineering Workshop - Decommission CHRONUS - PI Interface to HSH PI Interface Migration - OpenSTLF to Forecast Migration - OpenSOM to SOM Planner Migration - MSSQL 2008R2 to PostgreSQL Conversion and Historical Data Backfill - Smart Card Evaluation - Factory Q/A Testing - VM Export - Remote Networking Integration Assistance - Site Acceptance Test (SAT) Planning and Preparation - Post-Cutover Problem Resolution and Assistance - System Documentation Updates At RPU: - Site Installation and Configuration - 5-Day SAT (Additional Testing on T&M Basis) - SAT Cleanup - Cutover Preparation - Feature Differences Operator Training Session - Execute Cutover	1	371,100.00	EA	US$ 371,100.00
Additional Site Acceptance Test Days Site Acceptance Test Days to be Billed as Incurred ($2,000 per day) Not to Exceed $10,000	1	10,000.00	EA	US$ 10,000.00
Project Implementation Subtotal:				**US$ 381,100.00**
Training				
Training - Units Sufficient for One Attendee of the Following OSI-U Courses: - G310: Forecast - S280: SOM Planner	2	545.00	UNITS	US$ 1,090.00
Formal Onsite Admin Training Up to 5 Attendees Up to 5 Days Topics Covered Include: - To be Determined by OSI and RPU	1	15,000.00	EA	US$ 15,000.00
Training Subtotal:				**US$ 16,090.00**
monarch™ Support Adders				
monarch™ Support Adder - Gold	1	3,225.00	EA	US$ 3,225.00
monarch™ Support Adders Subtotal:				**US$ 3,225.00**

Open Systems International Inc.
4101 Arrowhead Drive, Medina MN 55340-9649
Phone: (763) 551-0559 Fax: (763) 404-4007
email: info@osii.com https://www.osii.com

Description	Qty	Unit Cost	Unit	Extended Cost
Travel				
Travel Travel to be Billed as Incurred Not to Exceed $22,500	1	22,500.00	EA	US$ 22,500.00
Travel Subtotal:				**US$ 22,500.00**
			Total:	**US$ 1,169,510.00**

Description	Qty	Unit Cost	Unit	Extended Cost
Option #1: 5-Year Custom monarch Support and Patch Management Renewal (Paid Annually)				
monarch™ Support				
monarch™ Support - Gold Support Period: 16-Nov-22 to 15-Nov-27 - Year 1: $118,619 - Year 2: $120,398 - Year 3: $122,204 - Year 4: $325,337 - Year 5: $125,898 - Technical Support - 24x7 - Help Desk - Unlimited Incidents - Webinar Training - License Assurance - monarch Upgrade Implementation in Year 4 Includes 3% Multi-Year Discount	1	812,456.00	EA	US$ 812,456.00
Discount:				**US$ -24,374.00**
monarch™ Support Subtotal:				**US$ 788,082.00**
Patch Management				
Patch Management Services - Gold Service Period: 16-Nov-22 to 15-Nov-27 - Year 1: $33,117 - Year 2: $33,614 - Year 3: $33,614 - Year 4: $34,118 - Year 5: $34,118 Includes 3% Multi-Year Discount	1	168,581.00	EA	US$ 168,581.00
Discount:				**US$ -5,057.00**
Patch Management Subtotal:				**US$ 163,524.00**
Option #1 Total:				**US$ 951,606.00**

Customer Address Info:

Bill To:
Riverside Public Utilities
PU - Elec Prod & Ops
Riverside CA 92504
USA

Ship To:
Riverside Public Utilties
2911 Adams Street
Riverside CA 92504
USA

Payment Terms:
Net 30 Days

Milestone Payment Details:
Base Quote
- 25% Upon Quote Acceptance
- 25% Upon Completion of Factory Q/A Testing
- 25% Upon Completion of Site Acceptance Testing
- 25% Upon Project Completion

Option 1:
- Year 1: 100% Upon Quote Acceptance ($147,184)
- Year 2: 100% Upon November 15, 2023 ($149,392)
- Year 3: 100% Upon November 15, 2024 ($151,143)
- Year 4: 100% Upon November 15, 2025 ($348,671)
- Year 5: 100% Upon November 15, 2026 ($155,216)

Special Terms and Conditions:

1. Any VM host hardware and workstation hardware supplied by RPU must be compliant with monarch™.NET minimum requirements as follows:
Minimum Host Server Specifications Per VM Instance*
CPU: 4 Physical Cores (8 Threads)
RAM: 16GB**
Disk IOPS: 150
OS: Windows Server 2012 R2, 2016, 2019, RHEL 7 or RHEL 8
Recommended Host Server Specifications Per VM Instance*
CPU: 8 Physical Cores (16 Threads)
RAM: 32GB**
Disk IOPS: 200
OS: Windows Server 2019 or RHEL 8
Required Workstation Specifications
CPU: Single Quad-Core HT, ~2.8GHz and above
RAM: 32+GB
Video Card: AMD Radeon Pro W5500 or better
OS: Windows 10 Pro 64-bit
*Quantities are additive, per VM (e.g. a host with 5 VMs will require 5x quantities shown). This does not reflect how to configure the VMs within the hypervisor; it is only a guideline for how to size the host hardware.
**In addition to indicated per VM RAM quantities, another 16GB RAM is required for the Hypervisor component.
2. All quoted hardware and third-party software licensing will be drop-shipped to RPU's facility. RPU will be responsible for spinning up new VMs and installing and configuring all third-party software (including OS). OSI will perform a remote OS inspection. Any issues found during the inspection will need to be resolved by RPU. RPU will then be responsible for sending all monarch VM's to OSI's facility via hard drives for monarch installation, configuration and testing.
3. RPU will be responsible for all installation and configuration for 3rd party VMs (i.e. Active Directoy, SCCM, backup/restore, antivirus, etc.). These will not be sent to OSI's faciltiy.
4. RPU will send OSI at least two (2) workstations for testing activities at OSI's facility.
5. RPU will ensure existing GPS antenna can be reused, or will handle procurement and installation of a new antenna, if necessary.
6. RPU will be responsible for modifying the monarch display for Time Deviation (i.e. deleting null values). It is recommended RPU uses the web user interface that comes with the GPS clocks.
7. OSI will convert and backfill up to five (5) years worth of historical data from MSSQL 2008R2 to PostgreSQL. Additional backfill and conversion efforts can be performed by OSI on a time and materials basis.
8. RPU will be responsible for all required network switch and firewall configuration.
9. RPU will participate in a 3-Day Data Engineering Workshop in which OSI will train RPU on the OSI Maintenance Server product. It is preferred that RPU travel to OSI for the Data Engineering Workshop. However, if RPU is not able to travel to OSI, the project plan can be reworked to accommodate for a remote Data Engineering Workshop.
10. RPU will provide all third party hardware, software, licensing, and configuration not specifically mentioned in this quote.
11. If required, RPU will handle any custom display and database work, and will test and verify all external links and interfaces. Displays and

databases are considered custom when more than minor adjustments are needed after the displays and databases have been converted over to the new version of monarch.
12. RPU will provide high-speed remote access to server and console hardware, if needed (VPN, Remote Desktop Connection, etc.). Dial-up modem connections are insufficient.
13. RPU will provide sufficient cabinet space for new hardware. If RPU is not able to provide this, additional cabinets can be quoted separately.
14. Project scope changes instigated by RPU (e.g. hardware quoted above being procured by RPU, etc.) may impact the project schedule.
15. A feature differences operator review session is included but limited to a brief hands-on, informal session. Additional training is included optionally.
16. OSI will perform a smart card evaluation to ensure monarch compatibility. RPU will be responsible for all other procurement, installation, configuration, testing etc. RPU will also be responsible for procuring keyboards with smart card support for the quoted workstations. The quoted workstations do not include keyboards. The quoted laptops have a smart card slot included.
17. Quoted SAT includes up to five (5) days of dedicated testing. Additional testing can be billed on a time and materials basis. Total dedicated testing will not exceed ten (10) days.

Standard Terms and Conditions

1. All quoted prices are in US Dollars ($), unless otherwise stated.
2. Travel and associated administrative costs are not included in this quote, and will be billed as incurred, unless otherwise stated.
3. Customer shall pay all applicable shipping and tariffs, unless otherwise stated.
4. Quoted price does not include applicable taxes, unless otherwise stated.
5. OSI will schedule all work upon receipt of the Customer's written acceptance, subject to OSI's resource availability.
6. Training, if applicable, will be provided at OSI's facility, unless otherwise stated.
7. Training Units may be used for up to 18 months from the date of purchase; any remaining unused Units will expire thereafter. One Training Unit is equivalent to one student attending one day of instruction for OSI University courses in Minneapolis (including Web-U courses).
8. Customer shall provide all relevant system information required for the work as needed (i.e. databases, displays, reports, IP addresses, networking information, RTU channel information, etc.) and shall be responsible for all delays caused by Customer's failure to do so in a timely manner.
9. Customer will have dedicated personnel available to assist OSI in the work, unless otherwise stated.
10. All third-party hardware purchased as part of this quote carries a standard OEM warranty, unless otherwise stated. All OSI hardware purchased as part of this quote carries a one-year warranty against defects from date of delivery, unless otherwise stated.
11. OSI does not guarantee that third-party goods will be available at time of quote acceptance. If third-party goods are not available, upon Customer's authorization, OSI will provide suitable replacements and bill any resulting cost differences to the Customer. Failure to timely authorize replacements may result in delays and/or need to re-quote.
12. When applicable, Customers subscribing to Gold or above Support Plans may be entitled to new software version updates without charge. With the exception of Diamond Plan subscribers, the Customer will be responsible to pay for any engineering services required to implement the software upgrades.
13. Unless otherwise agreed and quoted, Customer is responsible for all preparations for OSI's installation of software, hardware or services and any post-installation compatibility testing and compliance issues.
14. Customer will provide adequate environmental and power conditions onsite, unless otherwise stated.
15. Cutover is defined as the quoted functionality being operational with no outstanding critical incidents.
16. Any Quote(s) for system upgrade services require(s) that at the time of actual implementation Customer has a valid premium monarch™ Support plan which includes software upgrade privileges and that the system size or scope does not change dramatically between the issuance of the quote and implementation of the service.
17. Customer Furnished Hardware and Software: Customer shall provide all required third-party equipment and software ("CFE") for the Project except for the OSI-provided equipment identified in this quote. Customer shall be responsible to timely deliver all CFE to OSI in compliance with the mutually agreed upon Project Schedule for integration with the OSI software. Customer shall pay all shipping and insurance costs both to and from OSI and shall be responsible for all CFE warranties.
18. Export Controls:
18.1. Customer represents: It is not a citizen, national, or resident of, and is not under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has prohibited export and that it is not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor is it listed on the United States Department of Commerce Table of Denial Orders.
18.2. Customer agrees that it will not export or re-export the Product(s), directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries nor to any entity so listed on any of the above mentioned lists.
18.3. Customer agrees that it will not use the Product(s) for, and will not allow the Product(s) to be used for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.
18.4. The requirements of 18.2 and 18.3 above apply to all Product(s) purchased or licensed to Customer from OSI, whether included in this quote or purchased or licensed previously.

Notice: OSI's quote is based upon Customer's acceptance of all applicable Terms and Conditions. Requests for additions to, deletions of, or different Terms and Conditions, may require a revised quote and/or additional costs or schedule delays.

Exhibit "C"
Key Personnel

EXHIBIT C: Key Project Personnel

Jeff Miller
Senior Manager
Project Engineering
Jeff.Miller@osii.com

Tori Beattie, PMP
Director
Project Management Office
Tori.Beattie@osii.com

Shawn Niebler
Senior Account Manager
Customer Relations
Shawn.Niebler@osii.com

Exhibit "D"
Software Support Plan

monarch™ Software Support Program Overview

Revision 7.0
August 2016
OSI-555-103-MRK

TRADE SECRET

This document contains confidential and proprietary information and trade secrets of Open Systems International, Inc. (OSI). The information contained herein shall be used solely by the Licensee's/customer's employees, consultants and/or contractors responsible for the operation and maintenance of OSI's System Software, or potential clients in evaluation of the OSI product(s), and shall not be disclosed to third parties or widely and arbitrarily distributed within the Licensee's organization without OSI's expressed written permission.

Use of this document is subject to the Software License Agreement and the confidentiality agreement executed between the Licensee and OSI.

INTERPRETATION GUIDE

This overview and its descriptions and definitions shall be interpreted consistently with the Contract under which the Licensed OSI Software was provided, the Software License Agreement, which governs its use and operation, and any other written agreements between the parties.

Revision History

monarch Software Support Program Overview

OSI-555-103-MRK

Date of Change	Rev. #	Details of Change	Author	Approval
April 1999	1.3	Revision	L. Leeson	B. Hoveida
May 2000	2.0	Revision	L. Leeson	B. Hoveida
Nov 2001	3.0	Revision	L. Leeson	M. J. Nye
Sept 2002	4.0	Revision	L. Leeson	M. J. Nye
April 2004	4.1	Revision	N. Johnson	M. J. Nye
April 2005	5.0	Added References to web-based support and training and updated contact information	N. Johnson	M. J. Nye
April 2005	5.1	Final Review	M. J. Nye	B. Hoveida
May 2006	5.2	Minor updates	J. Richards	B. Hoveida
April 2007	5.3	Update references to Customer Relations. Add information regarding security services and Patch Management Program.	L. Leeson	B. Hoveida
August 2007	6.0	Update support plan level information.	L. Leeson	B. Hoveida
February 2009	6.1	Minor updates.	G. Meulemans	B. Hoveida
October 2011	6.2	Updated Customer Support Information	N. Masters	N. Masters
Sept 2012	6.3	Added OSI-PEDIA information	A. Hayden	P. Tsuchiya
Sept 2014	6.4	Added Remote System Access section	R. Tetzlaff	L. Leeson
August 2016	7.0	Updated remote access, support levels and trade secret language. Added life cycle information, TAM definition, definition section, new service features. Added "Interpretation" language to address differences between this document and individual contractual agreements.	L. Leeson	A. Halimah

Table of Contents

1 Overview 1

2 monarch Software Support Programs 3

2.1 Copper Support Program 3

2.2 Bronze Support Program 3

2.3 Silver Support Program 3

2.4 Gold Support Program 3

2.5 Platinum Support Program 3

2.6 Diamond Support Program 4

2.7 Support Program Levels 4

3 monarch Software Support Components 5

3.1 Remote System Access 5

3.2 Maintenance/Problem Fixes (All Levels) 5

3.3 Member Secure Portal (All Levels) 5

3.4 OSI-PEDIA Knowledgebase (All Levels) 6

3.5 Business Day Support (Bronze Level and Above) 6

3.6 Help Desk (Silver Level and Above) 6

3.7 After-Hours Support (Gold Level and Above) 6

3.8 Web-Based Training (Gold Level and Above) 6

3.9 Software Subscription/Updates (Gold Level and Above) 7

3.10 Unlimited Support Incidents (Platinum Level and Above) 7

3.11 On-Site Installation Assistance (Quotable or Diamond Level) 7

3.12 How Are Incidents Defined and How Does OSI Respond? 7

4 System Sizing and Complexity 9

4.1 Pricing 9

4.2 Partnership 9

4.3 System Complexity 10

4.4 monarch Platform Lifecycle and Support 10

5 Frequently Asked Questions 13

6 Best Practices: Preventive Maintenance 19

7 Definitions 21

8 Contact OSI 23

1 Overview

Mission Statement

Customer Support's mission:

- Help you achieve and maintain the highest level of system availability (better than 99.95%)
- Be a reliable technical resource to you to ensure your investment in OSI technology provides the highest return
- Work with you to ensure "change" is planned properly to maintain the highest level of reliability
- Facilitate your engineering and professional services needs above and beyond Support within OSI

Open Systems International, Inc. (OSI) offers one of the best software support and maintenance programs in the industry with a greater than 97% customer satisfaction rating. This document describes the features of the OSI customer support program for **monarch** software products.

General Features

OSI has a comprehensive and flexible set of support components to meet various customer needs.

- Tiered service levels for various size organizations and with tiered price levels.
- All support is NERC compliant and is conducted by OSI USA-based Engineering staff.
- Dedicated department, support staff, and assigned Technical Account Manager ("TAM") for handling incoming support calls.
- Access to OSI Member Secure Site and Secure Support portal.
- Gold level and higher support programs include **monarch** software subscriptions and software updates, 24 X 7 support and web training.
- Software subscription allows OSI customers to stay updated with the latest releases and enhancements. This leads to a very favorable lifetime cost of ownership.
- Web-based Customer Support tool

The following sections describe OSI **monarch** software support programs in more detail.

2 monarch Software Support Programs

OSI's standard **monarch** software support programs are described in the following subsections. These support programs combine various support components, as defined in Section 3, to devise a customized and cost-effective support plan for customers with various needs or budgets.

2.1 Copper Support Program

The Copper Support Program includes resolution of software deficiencies via software patches. This program does **not** include business-hour or after-hours support. This program does **not** include updates to new releases of licensed OSI software.

2.2 Bronze Support Program

The Bronze Support Program includes standard business-hour support service for up to 40 incidents per year. This program does **not** include after-hours service **nor** does it entitle you to receive new releases of licensed OSI software.

2.3 Silver Support Program

The Silver Support Program includes standard business-hour support service for up to 80 incidents per year and business-hour Help Desk service. This program does **not** include after-hours support service **nor** does it entitle you to receive new releases of licensed OSI software.

2.4 Gold Support Program

The Gold Support Program includes standard business-hour support service, help desk support, plus after-hours support service 24 hours a day, seven days a week for up to 80 incidents per year as well as access to OSI's web-based training program. Included in this program is the right to receive annual releases of the applicable licensed OSI software (in electronic format) for your system. Installation services are not included as part of this program and are purchased separately. OSI will quote engineering services for an upgrade plan tailored to your specific needs.

2.5 Platinum Support Program

The Platinum Support Program includes unlimited support service during business hours and after-hours. Platinum Support also includes standard help desk service as well as access to OSI's web-based training program. Included in this program are new releases of the applicable licensed

OSI software (in electronic format) for your system. Installation services are not included as part of this program and are purchased separately. OSI will quote engineering services for an upgrade plan tailored to your specific needs.

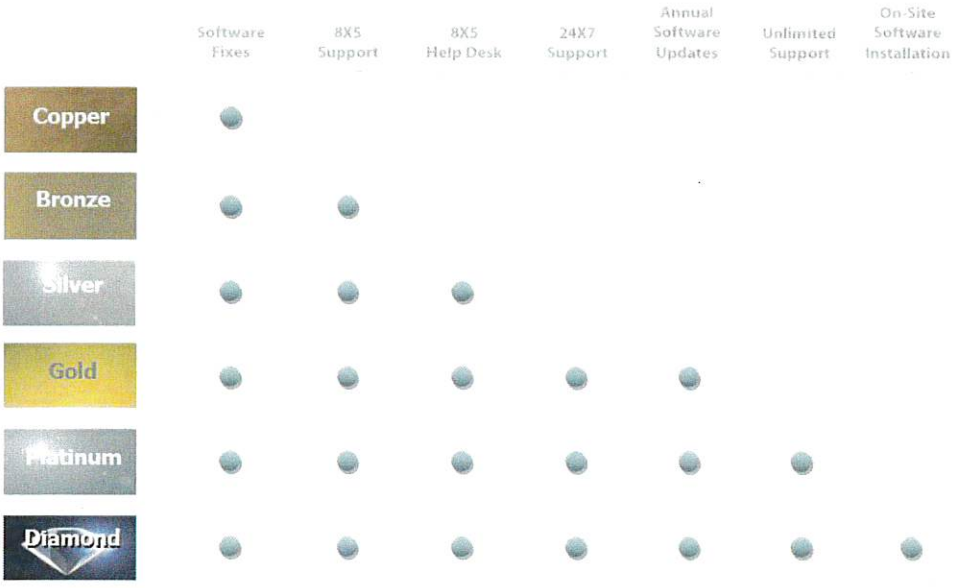
2.6 Diamond Support Program

The Diamond Support Program includes unlimited support service during business hours and after-hours. Diamond Support also includes standard help desk service as well as access to OSI's web-based training program. Included in this program are new releases of the applicable licensed OSI software along with on-site installation assistance once per year. Note: This does not include the costs associated with travel to the customer site.

Diamond Support can be a convenient and price-effective option for customers who wish to reduce budget review and approval cycles or include upgrade engineering services in an annual budget.

2.7 Support Program Levels

The following chart depicts the levels of service and the support coverage provided in each support program.



Customized support plans can be built by adding components, as needed, to your base support program. This allows you to select only those services that will most benefit your company.

3 monarch Software Support Components

The following components or building blocks make up the various **monarch** software support programs. These components are described below.

3.1 Remote System Access

OSI can remotely connect to your **monarch** system using secure methods. In order to ensure your system's security, meet regulatory requirements and keep our support infrastructure well-maintained and secure, we offer remote support using a fully-vetted set of Web-based screen share solutions that meet requirements of connection methods, technical quality, market acceptance and administrative overhead. We are very committed to ensuring the security of your system. Remote access is not a requirement for system support but can assist with the rapid resolution of important issues. See the *OSI Cyber Security Manual* or Cyber Security Portal for information regarding currently supported remote access tools.

OSI currently supports and recommends two remote access tools:

- Bomgar Remote Support Software
- Cisco AnyConnect (latest version)

Note that as regulatory requirements, customer needs and technology advancements change, OSI will periodically review and revise supported remote access methods.

3.2 Maintenance/Problem Fixes (All Levels)

OSI will fix reported OSI software deficiencies and provide software patches and/or workarounds for reported problems. This is limited to the maximum number of incidents allowed by your program. *This is comparable to an extended warranty service for a product, giving you a mechanism to obtain* **monarch** *software patches for software issues you encounter.*

3.3 Member Secure Portal (All Levels)

This is the launch point for access to product information, discussion groups, the support portal, the **OSI-PEDIA** knowledgebase, Support and CRG chat, and newsletters.

3.4 OSI-PEDIA Knowledgebase (All Levels)

This contains short articles regarding common support incidents, Frequently Asked Questions, tips and tricks, and additional references to product documentation.

3.5 Business Day Support (Bronze Level and Above)

This component allows you to call OSI during business hours for assistance with resolving critical and non-critical deficiencies with **monarch** software operation. This is limited to the maximum number of incidents allowed by your program. *This is comparable to remote support for service requests in dealing with software issues encountered during normal office hours (8 a.m. to 5 p.m. CT).*

3.6 Help Desk (Silver Level and Above)

OSI will provide assistance with non-critical issues and problems and provide general advice and guidance on software operation. This service is available during OSI business hours only. This is limited to the maximum number of incidents allowed by your program. *This is comparable to help desk for non-emergency service requests when dealing with software issues or questions encountered. OSI will process these requests on a first-come, first-serve basis and will schedule a "one-on-one" private session with a Technical Support Engineer based on a mutually acceptable time.*

Please be advised that this service is not intended as an all-inclusive "Professional Services" program, general consultation services for implementation of projects, engineering of new functions or engineering of new applications, cyber security questions, nor is it a consultation service for non-OSI software related issues. It is solely a help desk service to answer questions on features of the implemented OSI software products or to assist in resolving software issues or problems. For other engineering requests, including requests for software upgrades, you are advised to contact OSI's Customer Relations group to obtain a Professional Services quotation.

3.7 After-Hours Support (Gold Level and Above)

Customers can call after business hours, during weekends and on OSI holidays for assistance with resolving critical problems with software operation. This is limited to the maximum number of incidents allowed by your program. *This is comparable to help desk for emergency service requests in dealing with software issues encountered after normal office hours (24/7).*

3.8 Web-Based Training (Gold Level and Above)

Web-based training is offered as a supplement to the **OSI University** training program. It is designed to enhance your Support experience with OSI and to refresh basic product knowledge. The courses provide in-depth and topic-specific training. OSI selects the topics based on customers' input and in areas where OSI feels supplemental training would help customers in configuration and maintenance of the software. Courses are open to enrollment on a first-come, first-served basis. Multiple sessions are normally scheduled to accommodate a large population of users.

3.9 Software Subscription/Updates (Gold Level and Above)

This is a software update subscription or software assurance service that entitles you to software updates free of relicensing charges. This subscription entitles you to receive the pertinent software updates to your licensed software once per annum

This subscription service is the most valuable part of the support program by far, as it insures your system against technical obsolescence and results in an "evergreen" system. Moreover, it allows an implementation approach in which the software can be upgraded periodically at a fraction of the cost, instead of having to replace the entire system and relicensing and repurchasing all of the software every 5–7 years.

Please be advised that the premium support programs offering the Software Assurance program are predicated on the customer being on a continuous service program with no lapse in service. A support program reinstatement fee is required when reactivating a lapsed premium **monarch** software support program as well as fees for reinstating the Software Assurance component.

3.10 Unlimited Support Incidents (Platinum Level and Above)

This option allows you to uplift your support program to an unlimited number of help desk, business day support and after-hours support incidents.

3.11 On-Site Installation Assistance (Quotable or Diamond Level)

The software subscription provides the right to receive the software updates and does not include any support or engineering services for installation of these releases or consultation on such installations.

The installation assistance component provides the engineering services to perform the upgrade on-site.

OSI personnel will check and certify the new software release with your database and configuration prior to site installation, install software upgrades on-site (upon your request) and assist during your cutover to the new release (travel and living costs associated with the trip are invoiced separately). This is a convenient option for customers who want to minimize internal budget review, approval processes and roll the cost of such services into a single budgeted annual support fee.

3.12 How Are Incidents Defined and How Does OSI Respond?

OSI defines an incident as any request for support or assistance with the **monarch** software. There are two levels of incident urgency: **critical** and **non-critical**.

Critical Incidents:

For any possible critical incident (loss of visibility, communications or controls; loss of Automatic Generation Control and so on) you should IMMEDIATELY contact Customer Support by phone, identify the situation as critical and determine the appropriate plan for resolution.

Critical incidents are those that inhibit essential software operation and/or result in a substantial loss of operational capability. Critical software problems may include: FEP/communications failure and loss of scanning, SCADA software failure, the loss of Automatic Generation Control or interchange scheduling functionality and critical ICCP data links among others. For critical incidents, your Technical Account Manager (TAM) or an on-call engineer will return your call promptly (generally within 30 minutes) and will work with to resolve the incident until it is resolved, a workaround has been provided, or you decide to continue at another time.

Non-Critical Incidents:

Non-critical incidents are divided into **urgent, non-urgent** and **help desk**, which includes **chat:**

- **Urgent incidents:** The system or product is operational but there is some risk to operational stability, productivity or the issue could have a serious business impact. For urgent submissions your TAM or an on-call engineer will return your call (generally within eight hours during normal business hours) and will work with you to assess the seriousness, resolve the incident or provide a workaround. **Urgent incidents should be submitted by a phone call.**
- **Non-urgent incidents:** include any problems related to system functionality that do not disrupt essential operations. Examples include minor software problems, or non-disruptive errors in user interface and displays. OSI provides a 24-hour response (Monday through Friday). Depending on the availability of our engineers, most requests will be responded to within the business week.
- **Help Desk:** system or product questions such as errors in documentation, questions related to how program functions work, help desk support and similar issues. OSI provides a 24-hour response (Monday through Friday) on all non-critical help requests and questions.
- **Chat:** this is an ideal tool for basic, single topic questions; quick double-checks and so on. OSI will generally respond immediately, although a follow-up time may need to be scheduled depending on the complexity and nature of the question.

4 System Sizing and Complexity

4.1 Pricing

OSI is a "product" company and it distributes its Standard Products to a large customer base. This results in extremely reasonable maintenance and upgrade costs. Application suite bundling allows more economical pricing than pricing individual applications. OSI also believes in a "partnership" approach to system support, where the customer is actively engaged in understanding and optimizing their system functionality while working closely with OSI.

The cost of each **monarch** software support program is based on the size, scope and complexity of the installed system, as well as the suite of OSI software applications within your system, support options selected, and the age and version of **monarch** and third-party software and components installed.

The following sections contain information about the factors that affect support pricing.

Upon request, OSI will quote support services that are not described in this document as part of a customized support program.

4.2 Partnership

OSI has found that customers who are engaged with their systems, are well trained, and who keep their systems current achieve the highest levels of reliability and satisfaction. In addition, the nature of a support relationship requires partnership in problem solving, effective communication and an understanding of all parties' roles. To resolve incidents as quickly as possible:

- Have trained staff available to work with OSI;
- Provide accurate and detailed problem descriptions;
- Be able to define any mitigating circumstances and changes to the system that may have contributed to the incident;
- Provide a clear statement of the operational impact and priority of the problem;
- Advise if there is a business or commercial impact associated with the incident;
- Be engaged in the problem correction and participate in resolution; and
- Communicate any change in priority/impact – keep us informed so we can respond accordingly.

4.3 System Complexity

In order to provide fair tiered pricing for the support programs, the programs are graduated for various levels of complexity and system sizes (for example, the number of Remote Terminal Units (RTUs) and/or database point sizes).

The following are common cost multipliers for specific system characteristics that may increase the scope of services and their associated pricing:

- Generation applications
- Network analysis applications
- Distribution management applications
- Operator training simulator
- UNIX servers
- Distributed client sites
- Split backup/servers
- Backup control centers
- Specials and custom applications
- Program development and quality assurance systems
- Pipeline network management applications

As systems sizing is expanded or additional software applications are added, the cost of a support program is impacted due to the increase in system complexity.

4.4 monarch Platform Lifecycle and Support

OSI uses an industry-standard release process that serves customers through scheduled and organized release cycles, which maintain backwards compatibility within versions and decouple applications from base releases. This allows applications to be installed and patched as needed, without requiring a version upgrade.

- **Premiere Release Period**: When a release becomes generally available, it enters the premiere release period. During the premiere release period, quarterly revisions enrich the release with major and minor enhancements and dedicated defect resolution. The release is available on the latest versions of OSI-supported operating systems and RDBMS.
- **Extended Release Period:** During the extended release period, OSI develops quarterly revisions to the releases for two years. These revisions introduce minor enhancements and resolve remaining software defects. To preserve release stability, extended support patches do not include major enhancements. After the release of the final extended support patch, the release enters the limited support period.

As with any software product, when system releases age more effort is required to deliver effective support and patch priority is affected by the number of installed systems. Note that older releases may experience increased support costs and/or less rapid patch releases.

- **Limited Support Period:** During the limited support period, OSI develops as-needed patches (at least twice) for the release for one year. Limited support patches resolve operationally critical defects and security issues. No other defects or enhancements are resolved in the Limited Support stage.
- **Sustaining Support Period:** During the sustaining support period, no regular revisions are scheduled. Specific revisions may be contracted on an individual, per-fee basis. After one year of sustaining support, the release enters the end of life period.
- **End of Life Period:** When the release reaches the end of life period, all support becomes "best effort." OSI no longer supports the release with any new development. Support is not available through the OSI help desk for end of life products. End of life dates are provided to allow ample time to plan and implement a **monarch** upgrade.

5 Frequently Asked Questions

What are OSI's standard hours of operation?

Standard business hours are 8:00 a.m. to 5:00 p.m. United States Central Time, Monday through Friday, excluding OSI holidays.

What are OSI's holidays?

OSI is closed on the following holidays. On these non-business days, our support staff is available to respond to *critical* incidents only.

- New Year's Day (January 1st)
- Memorial Day (Last Monday in the month of May)
- Independence Day (July 4th)
- Labor Day (1st Monday of September)
- Thanksgiving Day (United States) (4th Thursday in November)
- The Friday after Thanksgiving Day
- Christmas Day (December 25th)

How do I know when my warranty will end or support program needs to be renewed?

For customers exiting warranty, OSI will contact you prior to the expiration of the system warranty to ensure that you are signed up for information, access to the support tool and other OSI sites, and to ensure your support contacts have the necessary access information.

Customers currently enrolled in a **monarch** software support program will be sent an invoice and a notice approximately 60 days prior to their renewal date. An OSI representative is always available to assist you in evaluating your current level of **monarch** software support and choosing the program that best suits your system.

I have new support contacts or am not sure if I'm taking advantage of all available services.

OSI will be happy to schedule a review meeting to discuss available services and best practices. Contact Customer Relations or Customer Support to schedule a call.

Who and how many persons can be designated as our support coordinators?

You can designate up to three (3) trained representatives from your company to serve as your official support coordinators. In order to resolve your support issues quickly and effectively, OSI requires that all support incidents solely originate with your designated support coordinators. For

larger or multi-site customers or unusual circumstances, please contact Customer Relations or Customer Support to schedule a call to discuss optimal coordinator staffing.

OSI requires each selected customer representative to attend OSI training for all licensed software. We want to ensure that the personnel requesting support or coordinating support for the customer are qualified and trained in OSI's software and platform technology. We also highly recommend that they keep their training refreshed in subsequent years.

What is a TAM?

A TAM is a Technical Account Manager assigned to your system. The TAM works with you so that he/she knows your system, can respond more quickly, and can provide useful information to project and technical teams performing other services on your system.

What is considered "above and beyond" software support?

OSI software support programs are expected to provide assistance with operational issues for software that has been implemented and certified by you and OSI. They are not designed to be a general services program to provide assistance and consulting for training, non-software-related issues or planning for expansion and augmentation of your present operational system.

Prior to expanding or augmenting system functionality (hardware, software, networking and so on), OSI recommends that you coordinate support in advance with the Customer Support Department. Depending on the scope, the work may be considered as additional system implementation and therefore, beyond the scope of our standard software support. For example, if a new function is being implemented post-warranty, additional professional services beyond ordinary support may be required. OSI has other specialist groups in the organization that are equipped to handle the engineering, consulting, and implementation services that are required to implement the new functionality. In such cases, please contact Customer Relations at customerrelations@osii.com to obtain proper advice and a quotation for additional professional services.

What should I do if I need support?

For any possible critical incident (loss of visibility, communications or controls; loss of Automatic Generation Control, etc.) you should IMMEDIATELY contact Customer Support by phone, identify the situation as critical and determine the next best steps for resolution and a return of standard system functionality.

Generally for non-critical incidents, your own designated support coordinator(s) should thoroughly investigate the problem and try to resolve it. If your support coordinator(s) cannot resolve the problem, they should contact OSI Customer Support. This process ensures that your support coordinators have the necessary background information about the problem when they contact OSI Support, which in turn will lead to a more timely resolution.

For **non-critical and non-urgent incidents**, please visit the OSI Support website (https://support.osii.com/) and submit your incident online. The OSI Support staff will investigate your support request and work with you until resolution.

For **critical and urgent incidents**, please ensure that you have as much information as possible regarding the scope and nature of the problem and are ready to discuss the problem with the OSI Support staff. We strongly recommend that you request support for critical and urgent incidents

via phone calls. OSI's Support staff will collect the pertinent information and open an incident for tracking and managing the issue until resolution.

It is very important that all requests for software support go directly to the OSI Customer Support Department. OSI cannot guarantee timely issue resolution if a non-support employee is contacted.

What are the main features of the OSI Customer Support website?

The OSI Customer Support website allows customers to submit new incidents, track the real-time status of outstanding incidents and obtain customized reports for all open and closed incidents. In addition, you can communicate with the OSI Support staff by using the Web Conversation feature.

What is the recommended method of communications relating to non-critical incidents?

OSI prefers the use of the Web Conversation feature in the OSI Customer Support website for communications relating to non-critical incidents. If necessary, emails intended for the Customer Support staff can be sent to Support@osii.com.

The Ticket Reporting online form, available on the OSI Support website, is a great tool to assist with collecting any required data. This will enable OSI Support to provide a quick response and accurate resolution.

Emails sent about an existing incident should include the incident number in the email subject line. Emails received that do not have an existing incident number in the subject line will result in the creation of a new incident. We also encourage you to use the conversation and communication module of the support portal instead of emails.

What are the support telephone numbers?

Business Hours

In North America, call 800-919-3997 during normal business hours. *If you experience problems reaching support at this number, please call* **866-205-6458** *directly as a backup number.*

Non-Business Hours

In North America, call **866-500-OSII (6744)** *during non-business hours. Support calls during non-business hours should be for loss of critical system functionality only. An on-call engineer will return your call promptly (generally within 30 minutes). If you experience problems reaching support at this number, please call* **866-205-6458** *directly as a backup number.*

For security purposes, please be prepared to supply your security code/support registration number for all support requests. OSI will notify you of your security and registration codes each year upon registration for support. Please safeguard these numbers and make them available only to your authorized support personnel. You can request new numbers for security purposes if there is a change in your staffing.

What number should I call if I am not in North America?

This will be determined upon your initial enrollment in the **monarch** software support program.

What information or details will be required for after-hours support calls?

When you contact OSI after-hours support, you will be required to provide an After-Hours Security Code. You will also be asked to define if the incident is critical. This information will be provided to the OSI on-call engineer.

What if I request services beyond the scope of my program?

If the number of allowed incidents in a year is exceeded, OSI will assess a charge of $1,000 per incident and $250 per hour (in USA dollars) for each additional request for support/incident beyond the coverage limits of the Bronze, Silver and Gold support programs.

Other services not included in the usual scope of coverage can be quoted as needed on a Time and Materials basis. You can contact Customer Relations or the Business Development Department at quote@osii.com for more information.

What if I did not purchase monarch Software Support or I need after-hours support with a Bronze or Silver Support Program?

If support services are needed, contact the Customer Relations group at customerrelations@osii.com in order to receive a quotation for these additional engineering services.

What is the industry norm for support costs?

The software industry norm for software support is usually 20% to 30% of the purchase price of the system per year. For example, if the software costs $100,000, the support for that software is typically $15,000 - $20,000 (minimum) per year. This does not include software updates or upgrades; these costs can run at an additional 10%-15% per year. OSI's proposed support costs are typically much more economical than the competitive industry programs.

What are the justifications for enrolling in the support program and how can I convince my management to purchase support?

There are five major needs filled by a support program:

- Extended Warranty and Insurance: an extended warranty that guarantees software fixes
- Guaranteed timely assistance from a vendor in case of critical needs
- A cost-effective method to ensure an "evergreen" system
- Improvements and enhancements are received with software updates, which defers future repurchases of software licenses
- Regulatory and market requirements often require the ability to demonstrate system availability and reliability

To estimate the cost savings your organization will realize, consider the additional staffing and training required to maintain the system or the cost associated with the purchase of new software due to new requirements, expanded sizing and so on.

What proficiencies does OSI recommend for staff?

OSI recommends that your employees have a four-year degree in Software or Electrical Engineering, a SCADA system background and have completed the required OSI training.

Employees working with power systems applications should also have power system/network modeling experience and a familiarity with power flow calculations and applications.

What would it cost my organization to provide self-support instead of purchasing support from OSI?

The support staff must be trained and (if after-hours needs exist) available around the clock. This is the core value and justification of the service OSI offers. The burdened cost of a single technical employee usually ranges from $120,000 - $150,000 per year. This cost does not include expenses, such as retraining and retention of staff or the added infrastructure and operational costs. To build an effective self–support infrastructure, a team of 2-5 people is usually needed. OSI support programs minimize the level of additional internal support staffing that is otherwise needed.

What can I expect to save using a premium software support program?

Software upgrades have an intrinsic value because your software investment does not become obsolete as time passes and technology changes. Assuming a ten (10) year life for a SCADA, EMS, DMS or GMS system, the new features included with software updates allow the customer to defer the replacement of the system, eliminate obsolescence and enhance operational value and cost savings. For these reasons, the software industry places a value of 15% to 20% per year of the cost of software licenses for the software updates.

What are OSI's internal costs for providing support to all its customers?

OSI requires an infrastructure to deliver our support services, which includes constant updates for hardware, software and networking. Our Development and Engineering staff will triage incidents, work on resolving problems and investigate future enhancements. Engineers are on staff to handle the probable load of support services and to manage emergency events. In addition, an organizational management structure is required to provide support to all customers. This is a costly endeavor and is the basis of our support costs to our customers. Overall, we believe our costs are very competitive in this market. OSI strives to manage internal costs in an effort to minimize the impact to our customers.

Does OSI offer multiple-year discount programs?

Yes! There are discounts available for multiple-year commitments that are paid in full at the onset of the support program. This lowers the cost per year of service.

Why can't I call the project engineers or the engineers that worked on my project for support?

In order for us to provide optimum and uniform coverage for all of our support customers, we must have dedicated support staff. The support staff is trained to deal with genuine support issues, while the project engineering staff is trained to deal with project implementation issues. Once a project enters warranty, the project engineering staff is allocated to other implementation projects and may be unable to provide timely responses.

Rest assured OSI uses all resources at its disposal including the original project engineers to address your support requests. It is imperative, however, that you continue to utilize the OSI Customer Support department for all support-related services.

Does OSI offer cyber security services or patch management services?

Yes. These are offered as optional services in addition to the Software Support programs. If you are interested please contact your Customer Relations representative at customerrelations@osii.com for additional information.

What additional assistance is available through Engineering Services?

OSI Engineering Services is available to fulfill a variety of needs. They can be utilized for customized training, advanced application development, product enhancements, system audits, cyber security audits, augmented staffing services and many other consulting needs. Please contact your Customer Relations representative at customerrelations@osii.com for additional information.

6 Best Practices: Preventive Maintenance

- Monitor system health - disk space, system resources, reviewing log files and so on
- Have a structured backup process
- Verify the OSI system configuration for consistent setup and use of the tools throughout multiple sites/systems
- **Regularly practice failovers (local and inter-site); preferably monthly**
  - Practice operating from the backup site for an extended period
  - Ensure that all relevant staff has a good understanding of failover processes - including providing operators with a process to manage while administrative staff are route
  - Educate staff on the criticality and impact of system outages – engage with OSI early in your triage process
- Ensure your staff is properly trained
  - Your trained staff should be available 24/7
  - OSI Support needs to work with your trained staff
  - As staff changes, new staff should be trained prior to assignment
  - Highly encourage refresher training for existing staff – especially with major upgrades where features are added
  - Take advantage of remote and free training and information resources available to support customers
- Keep your system up-to-date
  - Leverage most recent product improvements
  - Align your system with other customers
  - This is often the easier path to correct an issue in a more current release via patching/updates, particularly for cyber security issues
- **Call us when in trouble - don't wait!**

7 Definitions

"Base"

The **monarch** operating system

Deficiency or Deficiencies

Any malfunction, error, problem, bug, or defect, or any combination thereof, in OSI software or any failure of OSI software to perform in accordance with the applicable specifications or which causes OSI software to fail to be operational.

Enhancement Request

An enhancement request is a feature or change that is not part of the current product release. It may be part of the product roadmap, which would be included in a future release or may be available as a custom option.

Licensed OSI Software

OSI-developed, machine-readable "object code" or "executable code" along with documentation (electronic or hardcopy) and media (tape, CD ROM, DVD and so on) licensed by the customer for use.

Operational

The condition where the licensed OSI software is substantially functional in accordance with the applicable warranties and specifications and usable for its purposes in the customer's daily operations and when all data has been loaded into the system and is available for the customer's use

"TAM"

The assigned Technical Account Manager

Versions

Software releases are called "versions" and use a four-part versioning number:

- Major versions iterate approximately every two years (similar to Microsoft Office). Major versions will include major enhancements and a complete release of the product.
- Major revisions/updates will occur at least once a year, depending on the life cycle of the release.
- Minor revisions will occur several times a year (quarterly).

- Patches will take place on an as-needed basis (possibly monthly for critical and security patches).

8 Contact OSI

Supporting Your System: Other Resources

OSI has a robust selection of services that allow you to select the perfect Support program for your technical and business needs. Contact Customer Relations if you would like more information regarding these services:

- Patch management services
- Security Profiler
- System health assessments
- System architecture reviews and planning
- Network model design, testing and optimization
- Professional services

Getting in Touch with OSI

OSI welcomes your input about all aspects of our product and service offerings. You may find the following email addresses useful:

- support@osii.com - Customer Support department
- quote@osii.com - Request sales or product information
- ideas@osii.com - Suggestions for improving products and services
- training@osii.com - **monarch** training and **OSI University** information
- sales@osii.com - General questions or information regarding new project needs
- customerrelations@osii.com - Customer Relations for general assistance
- webmaster@osii.com – Information regarding the Member Secure Site

We make every effort to respond promptly to all questions and provide the help or information you need. Customer Relations will also be glad to assist you in any way they can. Customer Relations is your internal advocate within OSI.

Exhibit "E"
Software License Agreement

OSI

SOFTWARE LICENSE AGREEMENT

This Software License Agreement ("Agreement") is made this ____ day of _____, 20__ ("Effective Date"), between Open Systems International, Inc., with offices at 4101 Arrowhead Drive, Medina, Minnesota, USA 55340-9457 (hereinafter "Licensor"), and City of Riverside, a California charter city and municipal corporation, with offices at 3900 Main Street, Riverside, California (hereinafter "Licensee").

1. Definitions.

1.1 "Software" means (i) the machine-readable, object-code version of Licensor's confidential and proprietary software, including Server Software and Client Software, as set forth in the List of Deliverables or any subsequent orders thereafter; (ii) the Documentation; and (iii) any updates or revisions that Licensee may receive.

1.2 "List of Deliverables" means the list of products and software purchased or licensed by Licensee.

1.3 "Documentation" means the user guides and specifications for the Software that are made available by Licensor in electronic or tangible form.

1.4 "Server" means any physical server and/or any virtual server created by logically partitioning a physical server to create multiple virtual platforms or systems within a single physical server.

1.5 "Server Software" means that portion of the Software, which is installed on a Server or on a redundant pair of Servers (i.e., 2 computers), which serves a number of simultaneous users in a production environment. Some systems may also be licensed with additional Server licenses for development and test environments as well as disaster recovery and emergency backup purposes which, if any, are defined in the List of Deliverables.

1.6 "Client Software" means that portion of the Software, which is physically or virtually installed on a single user workstation or computer, which allows connection with the Server Software and use of the Software.

2. License Grant/Use of Software.

2.1 Grant of License. Licensor hereby grants to Licensee, pursuant to the following terms and conditions, a perpetual, non-exclusive, non-transferable, license to use the Software in support of its primary business mission and in operation of its own assets.

2.2 Permitted Uses. Licensee may:

(i) Transfer the Software to other equipment if the particular primary equipment is inoperative, provided that at any time the Server Software and/or Client Software are active in accordance with the number of licenses purchased.

(ii) Make static archival copies of the Software, provided that such copies shall include Licensor's copyright and other proprietary notices. All copies made by Licensee are the exclusive property of Licensor. At no times shall this copying create an unlicensed replication of the Software for use on unauthorized computers.

(iii) Make copies of the Documentation, provided that such copies shall be used only for Licensee's internal purposes and are not republished or distributed beyond Licensee's premise. Such copies shall include Licensor's copyright and other proprietary notices.

(iv) Develop applications in support of its business using the Licensor-provided Application Programming Interfaces (APIs) and tools delivered with the Software. Such Licensee-developed new applications are not considered part of Licensor's Software.

2.3 Uses Not Permitted. Licensee may not:

(i) Copy the Software, except as permitted above.

(ii) Transfer, sublicense, distribute, pledge, lease, rent, share, sell, lend or otherwise transfer all or any portion of the Software.
(iii) Translate, modify, adapt, decompile, disassemble, or reverse engineer any Software, in whole or in part, or to bypass any licensing restrictions.
(iv) Modify or create unauthorized derivative works of the Software or Documentation.
(v) Use the Software to provide software services through remote hosting or otherwise, or to process the data of a third party or any other use of the Software for commercial gains.
(vi) Install the Software on computers not owned, leased or otherwise controlled by Licensee, unless the License expressly allows installation on commercial third party cloud infrastructure.
(vii) Create multiple-use operations or multiple hosting facilities above and beyond the number of environments expressly licensed by installing the Software in more than a single physical or virtual location to allow simultaneous and parallel use of the Software.
(viii) Create images of the Software on virtual servers to override or bypass the number of required licensed copies, or to create back up control centers or hot back up sites for disaster recovery by not licensing these Software extensions to the license from the Licensor.

2.4 Use on Designated Equipment. Licensee agrees to:
(i) Install the Software only on computers owned, leased, or otherwise controlled by Licensee, unless the license expressly allows installation on commercial third party cloud infrastructure instead of on premise computer infrastructure.
(ii) Limit the use of Server Software to physical or virtual sites consistent with the number of Server Software licenses purchased as listed in the List of Deliverables. Any installed instance of the Server Software on a physical or virtual server shall be counted as an instance and shall be consistent with the number of licensed copies.
(iii) Only install the Client Software on single workstations or single personal computers and in accordance with the number of Client Software licenses purchased as listed in the List of Deliverables.

3. License Fees/Audit.

3.1 In consideration for the foregoing license, Licensee shall pay Licensor in full for all applicable license fees as set forth in the associated order(s).

3.2 During the term of this Agreement, Licensor shall have the right, from time to time, upon thirty (30) days advance written notice and at its expense, to direct a recognized accounting firm to conduct, during normal business hours, an audit of (and to copy) the appropriate records of Licensee to verify the number of physical or virtual copies of the Software in use by Licensee, the computer systems on which such copies are installed and in the case of limited user licenses, the number of users using such copies, and the database sizing dictating the database size-dependent license fees. If an audit reveals that Licensee has underpaid fees to Licensor, Licensee shall be invoiced for such underpaid fees based on Licensor's readily ascertainable prices in effect at the time the audit was completed. Representatives of the accounting firm shall protect the confidentiality of the Licensee's Confidential Information and abide by the Licensee's reasonable security regulations and conduct themselves in such a manner as not to interfere unreasonably with Licensee's normal business operations while on Licensee's premises.

4. Warranty.

4.1 Scope of Warranty/Warranty of Title. Licensor hereby represents and warrants that: (i) Licensor has good and marketable title and the right to license the Software free and clear of all liens, security interests and encumbrances; and (ii) the Software does not infringe upon any U.S. patent, trademark, copyright, trade secret or other proprietary right of any third party. Any warranties against defects are set forth in the contract for services between the parties.

4.2 EXCEPT AS SET FORTH IN THIS SECTION 4, LICENSOR MAKES AND LICENSEE RECEIVES NO EXPRESSED OR IMPLIED REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE SOFTWARE, ITS CONDITION, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE OR USE BY LICENSEE. LICENSOR FURNISHES THE ABOVE WARRANTIES IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY

AND FITNESS FOR A PARTICULAR PURPOSE AND ALL SUCH EXPRESS OR IMPLIED WARRANTIES ARE HEREBY DISCLAIMED.

5. **Limitation of Liability.** Neither party shall be liable, whether in contract, warranty, tort (including negligence), strict liability, indemnity or any other legal theory, for indirect, special, incidental or consequential damages, however caused, including but not limited to, any such damages arising out of the use or operation of the Software, delays in delivery or repair, loss of use of the Software, or damage to any documents, data or other property of Licensee, loss of revenue or profit; for costs of capital or of substitute use or performance; or for any other loss or cost of a similar type; or for claims by either party for damages claimed by the other party's customers. Except in the case of gross negligence, reckless or willful misconduct, claims of personal injury or property damage, or a breach of Confidentiality (under Section 7) or a breach of Intellectual Property Indemnification (under Section 6.2), the maximum liability under this Agreement shall not exceed the total license fees paid under this Agreement.

   Both parties agree that the exclusions and limitations set forth in this Section 5 do not preclude either party from obtaining equitable or injunctive relief or pursuing others who may be responsible for some or all of any losses incurred.

   Licensee acknowledges and agrees that Licensor has set its prices and entered into this Agreement in reliance upon the disclaimer of warranty and limitation of liability set forth herein, that same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

6. **Intellectual Property Rights and Indemnification.**

   6.1 Proprietary Rights. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to the Software are and will remain the property of Licensor or its licensors, whether or not specifically recognized or protected under local law. Only Licensor shall have the right to modify, maintain, enhance, or otherwise alter the Software source code, unless specified otherwise.

   6.2 Intellectual Property Indemnification. Licensor shall defend any claim, suit, or action filed against Licensee, its directors, officers, employees, agents, contractors, successors and assigns to the extent based on an allegation that the Software, as of its delivery date to Licensee, infringes any third party's valid U.S. patent or copyright. Licensor shall indemnify Licensee from any adverse final judgment (or settlement to which it consents) relating thereto.

   Notwithstanding the foregoing, such indemnification obligations shall not apply: (a) unless Licensor is given prompt written notice of any claim or threat after Licensee learns of such claim or threat and such information and assistance as Licensor may request in order to prosecute its defense; and (b) unless Licensor is given the opportunity to control the defense of such action, provided however, that Licensee shall have the right to approve papers filed regarding dispositive motions and shall have the right to approve any settlement of any claims brought against it; (c) if the Software involved has been altered in any way by Licensee or other(s) and such infringement would not have been alleged but for the alteration; and (d) if Licensee continues to use the Software after Licensor notifies Licensee to discontinue such use due to a filed or impending claim, suit or action. Licensee shall protect Licensor to the same extent Licensor has agreed to protect Licensee herein if a claim or a suit is brought against Licensor based on such alteration by Licensee.

   In the event any such infringement, claim, action or allegation is brought or threatened against Licensee, Licensor may, at its sole option and expense: (i) procure for Licensee the right to continue using the Software, (ii) modify the Software so as to be non-infringing, (iii) procure a replacement product that has substantially the same functionality, or if none of the above options are reasonably available, or (iv) terminate this Agreement by notice to Licensee without further obligation or liability to Licensee relating to such infringement.

7. **Confidentiality.** Each party agrees that should a party (the "Disclosing Party") share information with the other party (the "Receiving Party") which is designated or marked as proprietary or confidential, or information which, under the circumstances surrounding disclosure ought to be treated as confidential by the Receiving Party

(hereinafter "Confidential Information"), the Receiving Party shall not disclose this Confidential Information to anyone or use this Confidential Information for any purpose independent of the fulfillment of this Agreement . The Receiving Party shall not use any Confidential Information to the detriment of the Disclosing Party and shall use efforts to protect the confidentiality of any such Confidential Information commensurate with those which it employs to protect its own Confidential Information. The Receiving Party will ensure that it enters into agreements with employees, consultants, agents, shareholders and any other who have or may obtain access to the Confidential Information to maintain such Confidential Information in confidence. Confidential Information shall not include information which is: a) rightfully in the possession of or known to the Receiving Party prior to the disclosure without an obligation to maintain its confidentiality, b) publicly known or becomes publicly known through no unauthorized act of the Receiving Party, c) rightfully received by the Receiving Party from a third party without obligation of confidentiality, or d) independently developed by or for the Receiving Party.

In the event the Receiving Party receives a subpoena or other validly issued administrative or judicial process demanding the production of Confidential Information previously provided by the Disclosing Party, or in the event that the Receiving Party receives a request for such Confidential Information under the California Public Records Act, California Government Code sections 6250 et seq, the Receiving Party shall promptly notify the Disclosing Party of this fact and tender the defense of or opposition to this subpoena or demand to the Disclosing Party. If the subpoena or demand is not timely limited, quashed or extended, the Receiving Party shall thereafter be entitled to comply with such subpoena or demand to the extent required by law. If requested by the Disclosing Party after the tender of defense or opposition is accepted, the Receiving Party shall cooperate in such defense or opposition at the expense of the Disclosing Party. For the avoidance of doubt, to the extent that a request is made under the California Public Records Act, California Government Code sections 6250 et seq., the Receiving Party's sole obligation is to promptly notify the Disclosing Party of the request.

The Parties acknowledge that unauthorized disclosure of Confidential Information in violation of this Section may result in irreparable harm for which monetary damages or other remedy at law may be inadequate. Each party shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper and necessary by a court of competent jurisdiction to prevent any irreparable harm which may be caused by a breach or threatened breach of this Agreement.

8. Termination.

8.1 Licensor shall have the right to immediately terminate this Agreement and the license granted herein:

(i) Upon written notice in the event that Licensee, its officers, agents, or employees materially breaches any provision of this Agreement. Such notice shall identify and describe the default upon which termination is based and the Licensee shall have thirty (30) days following receipt of the written notice to cure such default.

(ii) In the event Licensee: (i) becomes subject to any bankruptcy or insolvency proceeding under Federal or State statute(s) which filing is not withdrawn within sixty (60) days for the filing thereof; (ii) becomes insolvent or becomes subject to direct control by a trustee, receiver or similar authority; or (iii) has wound up or liquidated Licensee's business, voluntarily or otherwise.

8.2 Upon termination, Licensee shall cease the use of the Software and either return or, upon request by Licensor, destroy the Software and provide a written affidavit to Licensor of the destruction of the Software. Termination under this paragraph shall not relieve Licensee of its obligations regarding confidentiality of the Software, nor relieve the Licensee of further claims made by the Licensor under the law for damages as a result of the violation of the terms of the Agreement. The provisions of Sections 5, 6, 7, 9, and 10, and any other sections that, by their terms, extend beyond the term of this Agreement survive termination of this Agreement for any reason.

9. Export Controls Compliance. Licensee agrees to comply with all applicable United States export control laws and regulations, as amended from time to time, including without limitation the laws and regulations administered by the United States Department of Commerce and the United States Department of State. Licensee agrees that neither the Software nor any data, information, program and/or materials resulting from Licensor's services (or any direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons

proliferation, or development of missile technology. Licensee will indemnify and hold Licensor harmless from any and all liability arising out of Licensee's use of the Software in violation of these laws, rules or regulations.

10. General Provisions.

10.1 Complete Agreement. Each party acknowledges that it has read and understands this Agreement and agrees to be bound by its terms. The parties further agree that this Agreement is the complete and exclusive statement of this Agreement between the parties, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties governing operation and use of the Software. This Agreement may not be modified or altered except by written instrument duly executed by both parties.

10.2 Waiver. The waiver or failure of either party to exercise in any respect any right provided for herein shall not be deemed a waiver of any other right hereunder.

10.3 Severability. If any provision of this Agreement is invalid, illegal or unenforceable under any applicable statute or rule of law, only that provision is to be deemed omitted and the remaining provisions shall not be affected in any way.

10.4 Assignment. Licensee may not assign the Software or this Agreement to anyone, including any parent, subsidiary or affiliate or as part of the sale of any portion of its business or pursuant to any merger, consolidation or reorganization without Licensor's prior written consent, except to a successor of all of Licensee's assets and business, provided the successor agrees to be bound by this Agreement and the successor is not a direct competitor of the Licensor. Licensee acknowledges that as a condition to such consent, Licensor may require the assignee to update all Software to the then-current version and purchase one year of Software support.

10.5 U.S. Government Contracts. Any Software or Documentation acquired by or on behalf of a unit or agency of the United States Government is "commercial computer software" or "commercial computer software documentation" and, absent a written agreement to the contrary, the Government's rights with respect to such Software or Documentation are limited by the terms of this Agreement, pursuant to FAR § 12.212(a) and its successor regulations and/or DFARS § 227.7202-1(a) and its successor regulations, as applicable. The manufacturer is Open Systems International, Inc., 4101 Arrowhead Drive, Medina, Minnesota USA 55340-9457.

10.6 Governing Law. The validity, interpretation, and enforcement of this Agreement shall be governed by the laws of the State of Minnesota, and the parties agree and consent to the jurisdiction of the State and Federal courts in: (1) Minnesota, USA, for any claim brought against Licensor by Licensee; or (2) Licensee's local legal jurisdiction (e.g., home state, province, country, etc.) for any claim brought against Licensee by Licensor. In the event of multiple claims, the first to file shall control governing law and jurisdiction as provided above.

10.7 Dispute Resolution. Any dispute for claims which will not result in irreparable harm if not immediately addressed may be brought for decision in the applicable court of competent jurisdiction only after the parties have met and attempted to amicably resolve the dispute.

10.8 Limitation of Actions Period. No action, regardless of form, arising out of this Agreement may be brought by either party more than twelve (12) months after the cause of action has arisen.

10.9 Counterparts. This Agreement may be executed in counterparts, all of which when executed and delivered shall constitute one single agreement between the parties.

SIGNATURES ON FOLLOWING PAGE

The parties are signing this Agreement as of the Effective Date.

Licensor:
Open Systems International, Inc.
4101 Arrowhead Drive
Medina, Minnesota USA 55340-9457

Licensee:

By: _____
(Signature)

Name: _____

Title: _____

Date: _____

By: _____
(Signature)

Name: _____

Title: _____

Date: _____

Exhibit "F"
OSI Cybersecurity Obligations

OSI CYBERSECURITY RISK MANAGEMENT REFERENCE DOCUMENT

This Cybersecurity Risk Management reference document describes how OSI will assist its customers in their compliance with applicable cybersecurity related laws and regulations, which may include the Critical Infrastructure Protection ("CIP") reliability standard CIP-013-1: Cybersecurity – Supply Chain Risk Management ("CIP-013") Requirement R1.2 relating to security controls for vendors. **This document is based on the Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk promulgated by Edison Electric Institute ("EEI").**

Definitions

The following definitions apply only to the terms and conditions in this Document:

"BES" means Bulk Electric System as defined by the North American Energy Regulatory Corporation (NERC) Reliability Standards Glossary of Terms (Glossary).

"CEII" means Critical Energy Infrastructure Information and/or Critical Electric Infrastructure Information as defined by the Federal Energy Regulatory Commission (FERC).

"OSI" means Open Systems International, Inc. in relation to supplying a product or service.

"Company" means the organization that acquires or procures a product or service.

"Confidential Information" means, for purposes of these terms and conditions, any and all information concerning Company and its business in any form, including, without limitation, the products and services provided under this Addendum, that is disclosed to or otherwise learned by OSI during the performance of this Addendum. Such information must be reduced to writing and clearly identified as confidential and/or proprietary.

"Disclosed" means any circumstance when the security, integrity, or confidentiality of any Confidential Information has been determined by OSI to have been compromised in any material fashion, which may include incidents where Confidential Information has been accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose.

"Restricted Information" means any Confidential Information that is additionally and clearly identified by the Company as Restricted Information under applicable statutes and/or regulations such as Company CEII or BES Cyber System Information (BCSI) information as defined by the Glossary. Company will only transmit such information via a mutually agreed secure mechanism. OSI will treat all Confidential Information, including Restricted Information, in a no less restrictive manner than it treats its own Confidential Information. OSI can agree to additional protections for specific information, but this may cause increases in scope, cost, and/or may require additional or different services agreements.

"Security Incident" means when OSI confirms that (1) Confidential and/or Restricted Information in the possession of the OSI has been Disclosed and such disclosure materially affects the Company Confidential Information, or (2) an incident has occurred that materially and adversely affects products and services provided by OSI.

1. Notification of OSI-identified incidents (Requirement R1.2.1)

OSI agrees to notify Company within 72 hours whenever OSI confirms that a Security Incident has occurred.

To the extent OSI is the cause of a Security Incident, OSI shall provide reasonable cooperation to Company in Company's efforts to determine the risk to the BES and to the Company posed by the Security Incident, including, upon written request from Company, providing additional information to the extent reasonably possible regarding the Security Incident. Company will designate a single point of contact who will lead their Security Incident investigation, and all such efforts will be coordinated with that individual.

2. **Coordination of responses to OSI-identified incidents (Requirement R1.2.2)**

Development and Implementation of a Response Plan: OSI shall maintain policies and procedures to address Security Incidents ("Response Plan") designed to (1) mitigate the harmful effects of Security Incidents, (2) remediate such Security Incidents, and (3) prevent the recurrence of Security Incidents in the future. The development, maintenance, and implementation of the Response Plan shall follow applicable industry practices.

Prevention of Recurrence: OSI shall develop a plan to reduce the likelihood of the same or a similar Security Incident occurring in the future, consistent with the requirements of its Response Plan, and shall communicate that plan to Company. OSI shall provide recommendations to Company on actions that Company may take to assist in the prevention of recurrence, as applicable or appropriate.

Coordination of Incident Response with Company: To the extent OSI is the cause of any Security Incident, as soon as possible and no later than 30 days of notifying Company of the Security Incident, OSI shall recommend actions to be taken by Company on Company-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as and to the extent deemed appropriate by OSI, the provision of action plans and mitigating controls. OSI shall take reasonable steps to coordinate with Company in developing mitigating controls and recovery efforts, to the extent the parties mutually determine such plans and controls are necessary.

Notification to Affected Parties: OSI will, to the extent it is the cause of any Security Incident, at its cost and expense, provide reasonable assistance and cooperation to Company's investigation of a Security Incident, and other remedial measures determined to be necessary by agreement of the parties in connection with a Security Incident.

In the event a Security Incident causes only Company Information to be Disclosed, such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of Company, under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by Company, with OSI's consent to the contents of such notice, except to the extent such notice is specifically required by applicable law or regulations. OSI's consent shall not be unreasonably withheld. The parties will mutually agree on the timing and method of providing such notification. OSI will directly notify appropriate governmental authorities, to the extent required by applicable law.

3. **Termination of Access Control of OSI Representatives (Requirement R1.2.3)**

Development and Implementation of Access Control Policy: OSI shall maintain policies and procedures

to address the security of remote and onsite access to Company Information, Company systems and networks, and Company property ("Access Control Policy") that is consistent with industry standard personnel management requirements, which may include ISO-27002, Section 9 *"Access Control"* and also meets the following requirements.

- Company Authority Over Access: In the course of furnishing products and services to Company, OSI shall not access, and shall not permit its employees, agents, OSIs, and other personnel or entities within its control ("OSI Personnel") to access Company's property, systems, or networks or Confidential Information without Company's prior express written authorization. Such written authorization may subsequently be revoked by Company at any time in its sole discretion. Further, any OSI personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Company. All Company authorized connectivity or attempted connectivity to Company's systems or networks shall be in conformity with Company's security policies as and to the extent provided to OSI prior to issuance of a contract and/or purchase order subject to these terms.

- OSI Review of Access: OSI will review and verify OSI Personnel's continued need for access and level of access to Company Information and Company systems, networks and property on a quarterly basis and will retain evidence of the reviews for two years from the date of each review.

- Company Review of Access: Company will review and verify Company Personnel's continued need for access and level of access to OSI Information and OSI systems, networks and property on a quarterly basis and will retain evidence of the reviews for two years from the date of each review.

- Notification and Revocation: OSI will immediately notify Company in writing at the email address identified in paragraph 1 (no later than close of business on the third business day as the day of termination or change set forth below) and will immediately take all steps necessary to remove OSI Personnel's access to any Company Information, systems, networks, or property when:

  (i) any OSI Personnel no longer requires such access in order to furnish the services or products provided by OSI,
  (ii) any OSI Personnel with unescorted physical or interactive access to Company BES cyber systems, as published in the "Access Permission Log" on the OSI's secure website, is terminated or suspended or their employment is otherwise ended (in such case, notification will be made within 12 hours of such termination or suspension by OSI),
  (iii) OSI reasonably believes any OSI Personnel poses a threat to the safe working environment at or to any Company property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or employee or Company Information, (in such case, notification will be made within 24 hours of such determination by OSI)
  (iv) there are any material adverse changes to any OSI Personnel's background history, including, without limitation, any information not previously known or reported in their background report or record,
  (v) any OSI Personnel fails to maintain conduct in accordance with the qualification criteria set forth in OSIs documented adjudication criteria.

(vi) any OSI Personnel loses their U.S. work authorization, or

(vii) OSI's provision of products and services to Company is either completed or terminated, so that Company can discontinue electronic and/or physical access for such OSI Personnel.

OSI will take all steps reasonably necessary to immediately deny such OSI Personnel electronic and physical access to Company Information as well as Company property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multi-factor security tokens, and laptops, as applicable, and will return to Company any Company-issued property including, but not limited to, Company photo ID badge, keys, parking pass, documents, or laptop in the possession of such OSI Personnel. OSI will notify Company at the email address identified in paragraph 1, once access to Company Information as well as Company property, systems, and networks has been removed.

4. OSI Vulnerability Disclosure and Remediation (Requirement R1.2.4)

OSI shall maintain policies and procedures to address the disclosure and remediation by OSI of vulnerabilities related to the products and services provided to Company including the following:

(a) Prior to the delivery of the procured product or service, OSI shall provide notice of publicly disclosed material vulnerabilities that have been mitigated in the procured product or services, the potential impact of such vulnerabilities, the status of OSI's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and OSI's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

(b) OSI shall follow a "Coordinated Vulnerability Disclosure" such as documented in ISO-29147 "Vulnerability Disclosure", NIST Cybersecurity Framework version 1.1. RS-AN-5 or NIST CSF. Possible mitigations may include a software patch/update, configuration change, procedural work-around, firewall policy change, etc. Vulnerabilities will be prioritized and mitigated according to their criticality in the applicable environment for the products and services provided, such as an Industrial Automation Control System environment.

(c) Prior to delivery of any system, OSI shall disclose the existence of all backdoors.

(d) OSI shall implement a vulnerability detection and remediation program consistent with applicable industry standards, such as ISO-27002 or IEC 62443-4-1 IACS Secure Development Lifecycle.

Disclosure of Vulnerabilities by Company: Company and OSI will agree on the manner, timing, and method by which any vulnerabilities or defects in the products and services provided by OSI are disclosed to any regulatory authorities with appropriate jurisdiction. Notwithstanding the foregoing, Company may make the minimum required disclosures required by applicable law or regulations without OSI's agreement, subject to any applicable confidentiality requirements or terms and conditions.

5. **Verification of software integrity and authenticity (Requirement R1.2.5)**

Hardware, Firmware, Software, and Patch Integrity and Authenticity:

(a) OSI shall maintain risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided to Company. OSI shall maintain documentation of its: chain-of-custody practices, inventory management program (including the location and

protection of spare parts), information protection practices, and integrity management program for components provided by sub-suppliers.

(b) OSI shall specify how digital delivery for procured products (*e.g.*, software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified by the mutually agreed specifications of any work provided by OSI. The parties will mutually agree to methods of encryption or other mechanisms to protect the digital delivery of products.

(c) For patches specifically provided by OSI, if OSI provides software or patches to its proprietary software (excluding any third party software) to Company, OSI shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from OSI's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of OSI.

(d) Upon written request, OSI agrees to comply with applicable laws specifically governing its procurement process, and agrees to provide an affirmative assertion, no more than once per calendar year, confirming its compliance with such laws.

(e) OSI shall use mutually agreed methods to ship procured products to Company, such as U.S. registered mail.

(f) The parties may agree to include a method for detecting unauthorized access throughout the delivery process and will include these requirements in the mutually agreed specifications.

(g) OSI may demonstrate chain-of-custody documentation for procured products as determined by mutual agreement of the parties which shall include tamper-evident packaging for the delivery of hardware.

Patching Governance for Products and Services Provided by OSI:

(a) Prior to the delivery of any products and services to Company and to the extent required by the mutually agreed specifications of any agreement, OSI will maintain its patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for OSI products, services.

(b) Procured products (including third-party hardware, software, firmware, and services) provided by OSI will have updates and patches installed prior to delivery to Company in accordance with the mutually agreed specifications of an agreement.

(c) Where and to the extent included in an applicable services agreement purchased by Company, OSI shall provide software and firmware updates to remediate newly discovered material vulnerabilities in its software (excluding third party non-embedded software) or provide workarounds for such vulnerabilities.

Viruses, Firmware and Malware:

(a) OSI will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to Company.

    (i) When installed files, scripts, firmware, or other OSI delivered software solutions are flagged as malicious, infected, or suspicious by an anti-virus program supported by OSI (e.g. McAfee, Symantec and Trend Micro), OSI will, to the best of its ability, provide technical background as to why the software should be considered a "false positive" to ensure their code's supply chain has not been compromised.

Cryptographic Requirements:

(a) Where and to the extent included in the mutually agreed specifications of any scope of work, OSI shall maintain documentation regarding how the mutually agreed cryptographic methods protect the confidentiality, data integrity, authentication. This documentation may include the following:
    (i) The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms).
(b) OSI will use the cryptographic methods detailed in the mutually agreed specifications of the work, which may include FIPS 140-. The foregoing statement does not require that OSI limit the cryptographic methods that any work provided by OSI may be capable of providing.

6. Coordination of Controls for Remote Access (Requirement R1.2.6)

OSI shall coordinate with Company on all remote access to Company's systems and networks.

Controls for Remote Access: OSI systems that directly, or through any of their affiliates, or service providers, connect to Company's systems or networks agree to the additional following protective measures:

(a) OSI will not access and will not permit any other person or entity to access, Company's systems or networks without Company's authorization and any such actual or attempted access will be consistent with any such authorization.
(b) OSI shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.
(c) For assets owned and/or controlled by the OSI, OSI shall ensure OSI Personnel do not use any virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any OSI or third-party systems, without prior approval of Company and ensuring that any computer used by OSI Personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Company systems or networks.
(d) OSI shall ensure individually assigned accounts are not shared between OSI Personnel.

7. Supporting Provisions

OSI Cybersecurity Policy: OSI will permit Company to review the OSI's cybersecurity policy at OSI's place of business or through mutually agreed virtual means, which shall be aligned with ISO-27001 as may be amended. For the avoidance of doubt, Company may not make copies of OSI's policies, which includes but is not limited to screenshots.

Return or Destruction of Company Information: Upon completion of the delivery of the products and services to be provided, or at any time upon Company's request, OSI will return to Company all hardware and removable media provided by Company containing Company Information. The hardware should be physically sealed and returned as mutually agreed by the parties. If the hardware or removable media containing Company Information is owned by OSI or a third-party, a written attestation detailing the date of destruction, will be sent to a designated Company security representative. OSI's destruction or erasure of Company Information pursuant to this Section shall comply with applicable industry practices.

8. Audit

Upon a written request from Company, the OSI shall provide reasonable evidence of relevant documentation, such as OSI's ISO-27001 security policies, procedures, evidence, and redacted auditor reports, that it determines, in its reasonable opinion, demonstrates OSI's compliance with the security related requirements of any agreement between the parties. If after review of the foregoing material, the Company identifies a security control required by any such agreement that is not addressed within the documentation provided by OSI, the parties will meet to determine a mutually agreeable approach to address Company's concerns.

If no such approach is developed, and the Company still determines, in its reasonable judgement, that an audit of OSI's controls specifically required under the contract for the protection of Company's data is required, OSI shall provide reasonable cooperation for the Company to perform an in-person audit of OSI. The scope of the audit shall be mutually agreed, but in any event limited to a document only and/or physical review of the security environment and procedural controls at the OSI's facility, excluding testing, to determine OSI's compliance with its contractual obligations specifically relating to the protection of Company's data. Company audits of the OSI location shall be performed by a mutually agreed auditor during normal business hours with at least 30 days' notice. Company is responsible for all costs related to such audit.

Exhibit "G"
OSI Patch Management Program

monarch™ Patch Management Service Plan Overview

Revision 2.2
March 2019
OSI-555-105-MRK

TRADE SECRET

Revision History

monarch Patch Management Service Plan Overview

OSI-555-105-MRK

Date of Change	Rev. #	Details of Change	Author	Approval
16OCT06	1.0	Initial Revision	B Rasefske	B. Hoveida
29DEC06	1.1	Revision	B. Hoveida	B. Hoveida
04JAN07	1.2	Final review and approval	B. Hoveida	B. Hoveida
10JAN08	1.3	Revision	A. Wortz	B. Hoveida
29JUL15	2.0	Updates for NERC CIPv5	R. Koziy	A. Halimah
6AUG15	2.1	FAQ updates; removal of sample agreement	R. Koziy	A. Halimah
15MAR19	2.2	Updates for entitlement changes; explanation of certification methodology	J. Brown	A. Halimah

Table of Contents

1 Overview 1
1.1 Patch Management Overview 1
1.2 Patch Management Justification 2
1.3 OSI's Patch Management Services 2

2 Patch Management Service (PMS) Components 5
2.1 What is OSI's Patch Management Philosophy? 5
2.2 What is Not Included? 6
2.3 PMS Service Levels 6
2.3.1 Operating System and Third-Party Product Certification 6
2.3.2 Help Desk Support 7
2.3.3 Web-based Training 7
2.3.4 Patch Management Service Benefits with NERC CIPv5 7

3 monarch PMS Programs 11
3.1 Silver PMS Program 11
3.2 Gold PMS Program 12

4 Deploying a Successful Patch Management Strategy 13

5 PMS: Legal Disclaimer 15

6 Frequently Asked Questions 17

1 Overview

This document provides a detailed overview of the Open Systems International, Inc. (OSI) Security Patch Management Service (PMS) program for **monarch** software products.

1.1 Patch Management Overview

Microsoft® defines patch management as "the process of updating your servers and desktops with the latest security patches and service packs." While this is sound advice, in today's computing environment, this involves much more.

Patch management is an integral part of protecting your corporate data and the operational integrity of your business mission. However, keeping systems up-to-date and compliant with security requirements is a complex endeavor due to:

- OEM (Original Equipment Manufacturer) Vendors releasing a large number of updates on a frequent basis
- Tracking and evaluating security risks and the appropriate software updates is time-consuming and requires in-depth knowledge of installed software, hardware and software dependencies and corporate requirements
- Deployment of patches must be managed carefully and methodically to reduce downtime or service interruptions
- Effective auditing and reporting is required to monitor deployment, verify compliance and troubleshoot errors

Classic patch management includes the following comprehensive processes:

1. "Vulnerability Awareness and Assessment" is concerned with auditing software in your production environment, evaluating potential security threats, vulnerabilities and non-compliances. It requires an accurate inventory of cyber assets to assess exposures.
2. "Patch Identification and Download" involves determining a reliable, timely source of information on software updates, and a documented and secure download process. Examples of software update sources include Microsoft Windows® Server Update Services (WSUS), Sun™ Update Connection, IBM® AIX Fix Delivery Center and the Linux® Red Hat Network.
3. "Patch Testing" includes validating the patches in a test environment and providing the assurance that all necessary packages, prerequisites, co-requisites and possible conflicts have been identified before deploying to the production environment.
4. "Patch Approval" is following a process to maintain strict control over what is being changed, which vulnerability is being addressed, what services and applications are being impacted, rollback plans and priority.

5. "Patch Deployment" includes prioritizing the urgency of the patch deployment, scheduling the deployment, distributing and installing the patch and rolling back on selected endpoints, if necessary.
6. "Patch Verification" is the validation that the patch was successfully applied to all of the target clients and servers.
7. "Compliance Management" includes updating the configuration baseline definitions to include the new patches and regular analysis of configuration changes to assure that all endpoints remain in compliance.

1.2 Patch Management Justification

The patching of system vulnerabilities has become one of the most labor-intensive and time-consuming recurring administrative tasks in the IT enterprise. The security patching process is further complicated by evolving NERC CIP regulations requiring NERC-regulated utilities to identify, test, install and document all security updates within a specific timeframe. The process is also prone to failure, as viruses and worms often use un-patched vulnerabilities as the initial entry point into a protected network and then use other techniques for propagating once inside. Thus, any of the following factors could invalidate the process:

- Patches that are not identified and installed in time to prevent damage
- Vulnerable systems that were not patched when the patch was deployed
- Defective patches that do not properly close the vulnerability
- Defective patches that create new vulnerabilities or cause loss of services

Furthermore, un-patched systems may present the following consequences to the enterprise as a whole:

- Costs and overhead associated with clean up after an infection or a security breach
- Direct loss of revenue from system outages and productivity declines
- Indirect financial loss due to loss of reputation and/or customer confidence
- Legal liabilities from breach of service to consumers
- System downtime
- Theft of business information assets

1.3 OSI's Patch Management Services

OSI has a comprehensive and flexible set of security patch management support components to meet various customer needs.

OSI provides support in certifying **monarch** software for security patches issued by various vendors of your operating systems and third-party/OEM software.

Your **monarch** software is tested and certified for operating system and third-party/OEM security patches in a baseline system. Certification is based on the U.S. Department of Homeland Security's Procurement Language for Control Systems and the NERC CIP requirements.

The following sections describe the OSI **monarch** Patch Management Service (PMS). The cost of a **monarch** PMS program is based on the operating systems used, scope of third-party software, scope and complexity of the installed system, as well as the suite of OSI applications within your system and the support components selected. OSI can also optionally quote support services that are not described in this document upon request as part of a customized patch management plan.

2 Patch Management Service (PMS) Components

2.1 What is OSI's Patch Management Philosophy?

Patch management is a general term used in the IT industry for managing platform and applications software security updates and software patches issued by software vendors. The NERC CIP standard and best practices requires you to establish and document a security patch management program for tracking, evaluating, testing and installing applicable cyber security software patches for all cyber assets within your Electronic Security Perimeter, including the platform software such as operating systems, relational databases and so on.

Third-party software vendors may issue hundreds of patches every year. Managing the applicability of these patches as well as the compatibility of these patches with your OSI **monarch** software could be a cumbersome task. For example, an OEM patch fixing a security hole in your RDBMS may have adverse effects on your running **monarch** software, breaking a required functionality that you may rely on.

OSI's security patch management services are intended to facilitate and assist you in the tracking of third-party security patches, determination of their applicability to your **monarch** software and the assessment of the potential impact of the security patch on your **monarch** system. Our patch management services will assist you in the following areas:

- Applicability

  OSI will determine and evaluate the applicability of the OEM security patch in relation to the core functionality of the **monarch** software, answering the question of whether the patch is applicable to your **monarch** software and system configuration.

  OSI will review all patches released for designated third-party products for security improvements, but will only report on updates with a security component or a prerequisite for a security update. All security patches included on OSI's certification report are considered to be applicable to OSI systems and should be installed or mitigated.

- Compatibility

  OSI will determine whether an applicable security patch will or will not interfere with the functionality of the **monarch** software and that the **monarch** software will run or will not run as before with the OEM patch installed. If the patch will interfere with your **monarch** software or impact **monarch** system operation, you will be advised to abstain from installing it until a corresponding compatible **monarch** patch is available from OSI. For offending OEM security patches that are critical to your system, OSI will attempt to provide a work-around or an OSI software patch to make sure the operation of your **monarch** system after the patch installation remains unchanged.

- Help Desk Support

  OSI will provide a Help and Support Desk to answer any questions on your patch installation of the OSI patches or any other questions related to your patch management activities and processes.

- Other Support and Services

  Optionally, as a separate quotable effort, OSI can provide you with engineering services and labor to install the OEM security patch as well as the OSI patch (if required), either through remote support or in some cases via on-site services. Additional customized services can also be provided for Security Audits as well as documentation and compliance reporting and so on.

2.2 What is Not Included?

For liability reasons, our services do not include certifying, testing or the offering of any guarantees that the OEM security patch itself will fix the offending security problem or that the OEM patch will work as advertised by the OEM. We may, however, share any pertinent experiences with you that we may obtain from working with the OEM patch on our test systems at OSI on an "as is" basis.

Security patches for OSI products are not part of the OSI Patch Management Service, and instead are communicated separately through the "Security Bulletin" area of the secure Member's website which is available to all OSI customers under the OSI Support program (i.e. OSI Patch Management Service is not required to receive these bulletins).

2.3 PMS Service Levels

In order to offer a cost effective program for various needs and budgets, we have devised a multi-level Patch Management Service (PMS) program.

PMS services cannot be offered independent of a premium **monarch** software support plan. For you to subscribe, you must be already under a **monarch** Gold Warranty, or a Gold, Platinum or Diamond support plan. Being on an active software support plan provides the basis for you to be able to receive OSI software updates (and patches to OSI software) if needed. If you are not on a premium **monarch** support plan and wish to subscribe to the OSI Patch Management Service, you first have to elect to subscribe to an OSI premium support plan (for example, Gold or higher).

Three standard components or building blocks make up each Patch Management Service program. These are described in the sections below.

2.3.1 Operating System and Third-Party Product Certification

OSI will test and verify that **monarch** software will continue to function as designed with operating system or third-party OEM software security patches installed.

OSI will consistently monitor, research and identify any new reported security patches or fixes associated with a registered third-party product. After identifying these patches, experienced OSI employees will begin analyzing the released patches and testing their impact on the appropriate **monarch** software releases.

OSI will promptly notify you (in a timeframe consistent with the level of service to which you have subscribed) of the applicability and compatibility status for current OEM-issued security patches.

OSI will use a secure Web portal for posting notice of the applicability and certification status. You will be responsible for checking the controlled website for these notices and independently deciding whether you wish to add a compatible patch to your system and, if so, to acquire and install the patch.

Certification does not include certifying, testing or the offering of any guarantees that the OEM patch will fix the offending security problem or that the OEM patch will work as advertised by the OEM. OSI may, however, share any pertinent experiences with you that we may obtain from working with the OEM patch on our test systems at OSI on an "as is" basis.

Certification completion is targeted as soon as possible after the OEM vendor release of their patches and consistent with the subscribed service level. The process involves evaluation and testing in OSI's production certification lab by a highly qualified software quality assurance group.

OSI also provides guidance to customers about the corrective actions, fixes or monitoring that is suggested to mitigate any vulnerabilities associated with the flaw.

The PMS Web portal is accessible via the secure area of the OSI Web site (http://www.osii.com/login/index.asp). You can visit this site and log in with your authorized user name to navigate to the Patch certification portal page of the secure site.

2.3.2 Help Desk Support

This component provides customers with phone support in the installation and verification of patches from experienced OSI staff. OSI will provide help desk support to answer any questions you have or to investigate any particular issue, up to your maximum incident levels designated for your PMS Service level. During normal business hours, help desk support will be provided through our Patch Management Service Coordinator, who can be reached via pms@osii.com or via phone at 763-551-0559.

Help Desk support will answer your questions regarding installation or talk you through the steps required to install a specific patch.

2.3.3 Web-based Training

Web-based training is offered to subscribers to demonstrate how customers can view patch management reports, export lists of certified patches based on various filters such as supplier, date certified, etc. .

2.3.4 Patch Management Service Benefits with NERC CIPv5

Patching requirements are changing for all utilities that fall under NERC jurisdiction. Table 2.3.4-1 below highlights the key differences in acceptable patching timeframes required by NERC version 3 vs version 5.

One very important change is the ability for a Utility to designate a "Patching Source" that is different than the original supplier of the software. Customers choosing OSI's Patch

management Services and designating OSI as their patching source allows their NERC required analysis and implementation periods to be extended. With OSI as the patching source, the "clock doesn't start" until OSI certifies the patch. With OSI Patch Management Service customer patching requirements are reset to the beginning of the release period provided by OSI, regardless of when the patch was released by Microsoft, Red Hat, Oracle, etc.

Summary of Benefits of OSI Patch Management Service with NERC CIPv5:

- Ability to designate OSI as the patching source for monarch and all related 3rd party software
- Additional time to perform analysis and implementation of patches - based on certification date from OSI (clock doesn't start until OSI certification date)
- Consolidation of multiple vendor release cycles into a single release cycle from OSI (eg. weekly, start/mid/end of month vs OSI 1st of month)

Description	CIP Version 3	CIP Version 5
Analysis period (based on date of release from patching "source")	30 days	35 days
Implementation period (based on date of validation from patching "source")	not specified - but 120 days from date of release has been accepted in audits	35 days
Source of patches	Defined as the original supplier (eg. Microsoft, Redhat)	Utility can designate a system vendor (eg. OSI) to be the patching "source"

Table 2.3.4-1

NERC CIP-007-5 Reference:

Wording which allows a utility to name OSI as the source is covered in the description of R2.1 within the "Guidelines & Technical Basis" section of CIP-007-5. See highlighted sections below.

CIP-007-5 R2.1 "Guidelines & Technical Basis . The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but

must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

3 monarch PMS Programs

OSI's standard **monarch** Patch Management Service programs are described in the following sections. These support programs include the components defined in Section 2 and devise a scalable and cost-effective support plan for customers with various needs and budgets.

These programs allow you to balance cost, your internal resource pool, administrative time for patch management and security by choosing an option specific to your needs.

In addition to choosing your program, you must also register specific computers, versions of operating systems and third-party products as well as **monarch** versions.

OSI's services may not cover all third party/OEM products installed on your system. Some applications (like system BIOS and other firmware, as well as applications that OSI does not procure or configure by standard) will not be available through this service. Customers can request that OSI evaluate its ability to add a new product to its portfolio. The evaluation will be performed at no charge. OSI cannot guarantee that it can support a product after the evaluation is completed. OSI will provide the customer with a quote for adding the application to its portfolio if it is determined that the product can be supported.

OSI maintains a list of products supported by Patch Management Services and your Customer Relations representative can provide this list upon request.

Patch Management service levels offered are:

- Silver PMS service
- Gold PMS service

Based on the service plan selected, subscribers will receive notification of certified patches at varying frequencies such as quarterly or monthly upon availability.

3.1 Silver PMS Program

The Silver PMS Program includes **quarterly** analysis and certification of **monarch** software for your registered third-party/OEM software. The Silver program provides for help desk support for up to **20** patch related incidents per year. Free Web-training is included as part of this service. Patch installation support or remote installation is available on an optional basis as a separate quotable effort.

Patch certification results will be made available each quarter and will include the certification dates for applicable patches from the Gold PMS Program.

3.2 Gold PMS Program

The Gold PMS Program includes **monthly** analysis and certification of **monarch** software for registered third-party/OEM software. The Gold program provides for help desk support for up to **40** patch related incidents per year. Free Web-training is included as part of this service. Patch installation support or remote installation is available on an optional basis as a separate quotable effort.

4 Deploying a Successful Patch Management Strategy

Ask an IT manager about the most pressing issues they deal with and chances are keeping their systems patched against security vulnerabilities is one of them. Regardless of which operating systems you use, patches are a fact of life, and keeping every system patched against all vulnerabilities is a never-ending task. Additional management and care are required in patch deployment policies when it relates to a critical control system. There are a variety of options to use for deploying these patches, ranging from manually patching each computer and device in your system, to a fully automated system that provides rule-based installation and reporting capabilities. However, there is more to effective patch management than just having the latest and greatest patch installed on a machine. Good processes and policies are essential for the success of any IT project, and patch management is no exception. Several tasks should be part of the planning portion of every patch management strategy you put into effect.

Develop a Written Patching Policy

Document all aspects of your patch management plan as a corporate policy, and make sure that all relevant employees are aware of the *who, what, how, where, when* and *why* of your organization's patching strategy, This policy should include at a minimum:

- Which systems will be patched
- How patches are prioritized
- The schedule according to which non-critical patches will be deployed
- The manner in which critical patches will be handled
- Required testing prior to deployment

Establish a Hot Team

The Hot Team responds to all newly identified critical patches. They put together a plan for action for the critical patches in accordance with the organization's patching policy, and oversee the execution of this plan. The team may also be responsible for continuous monitoring of security and patch information sites. It is a good idea to create a standard list of sources of patching information that will be relevant to your organization, and define the frequency that these resources are reviewed. This team will be the interface with OSI's Patch Management group.

Create Formal Change Control Processes for Deployment

Using formal change control processes for patch deployment is important for a number of reasons. First, your organization has a repeatable standard process by which a patch is physically rolled out, making deployment easier for the maintenance staff. Second, it is not uncommon for a patch installation to be problematic. A back-out plan is an essential part of any change control

process. Communicating in advance to the patching team what needs to be done when things go wrong can help keep outages to a minimum.

As stated before, there is more to patch management than just patching systems against vulnerabilities. The systems must also continue to serve their intended functions. Specific actions taken when rolling out patches can cause a loss or reduction of service to your end-users. An outage resulting from an un-patched vulnerability and an outage resulting from a patch rollout gone wrong are logically the same – an outage is an outage.

Document the policies and processes in each of these areas and incorporate them into standard operating procedures for your organization. Just by defining these areas, previously overlooked functional or non-functional requirements for the overall patching plan may be revealed and therefore make your entire strategy that much more effective.

Recognize the Risks

Security and business continuity issues consistently make headlines in the business pages. In one survey, 87% of businesses fear that another massive blackout will disrupt their operations. Then there are critical vulnerabilities to deal with, such as Havex, POODLE, OpenSSL. There does not appear to be any sign of a slowdown. The numbers speak for themselves:

- Provider networks receive 120,000 alerts per day
- Average time to impact of a vulnerability is six days (previously six months)
- Average of seven new vulnerabilities per day that must be dealt with
- 96% of threats are moderate or highly severe
- USA ranks first based upon attacks targeted for cyber infrastructure
- A major patch is released every six minutes

Plan to implement a Patch Test System

Your patch management burden will be minimized and your risks of installation will be better mitigated if you deploy your patches first on a non-critical and non-operational system. We recommend implementing a test system for patch management that is functionally a mirror image of your production **monarch** system. Many companies are implementing a quality assurance and test system based on NERC recommendations. This is in addition to a Program Development System (PDS) you may already have. OSI will be happy to assist you with planning and implementation of your Patch Test System. Please contact your customer relations representative if you require assistance.

5 PMS: Legal Disclaimer

OSI's service and certification is limited to a determination of whether the available third-party software security patch is compatible with OSI's **monarch** software products or will cause OSI's **monarch** software products to break down or fail to function properly. OSI makes no representations or warranties and assumes no liabilities regarding whether the security patch is necessary for or applicable to your specific system configuration, includes any defects or vulnerabilities or will enhance the security, performance or reliability of your system.

OSI will use its best efforts to determine and certify the compatibility of the security patches with OSI's **monarch** software products in a professional manner based on the industry's best practices. The OSI test platforms used for patch verification are representative of PMS customer systems, but may not match in every aspect or use. OSI software architects analyze 3rd party software to determine the required test plan. Should OSI be unable to certify compatibility between a necessary patch and OSI's **monarch** software products, OSI shall endeavor to develop the proper compatibility and will notify you on a timely basis if and when the compatibility can be provided. Neither OSI's liability nor your available remedies shall be increased by the patch management services offered, beyond that specified in your OSI Software License Agreement or Support Services Agreement.

6 Frequently Asked Questions

What is OSI's certification methodology?

OSI certification methodology is based on the U.S. Department of Homeland Security's Procurement Language for Control Systems and the NERC CIP requirements. **monarch** software will be tested and certified for operating system and third party/OEM patches on the latest releases of the baseline system.

What will the PMS service cost?

Cost is dependent on many factors and will be determined by evaluation of the following criteria:

- **monarch** Software version used
- Number of OSI products installed on your system
- Operating system(s) version(s) used
- Number of servers, workstations and complexity of operation
- System size in terms of points, RTUs and so on
- System complexity in terms of backup systems, DTS, PDS and so on
- Existence of a Quality Assurance System or Program Development System for testing purposes to facilitate patch management/installations

Can OSI assist me in the installation of my third party patches?

Three options are available for installation of patches:

- ***Help Desk:*** You will take responsibility for installation. You can call our help desk for questions or support using your allocated incident credits for the year. (This is offered as part of the base program at no additional costs to you.)
- ***Remote Support:*** Optionally, OSI staff will install your patches via remote connection for an hourly engineering charge.
- ***On-Site Support:*** Optionally, OSI staff will come to your site to install your patches for an hourly or daily charge and associated travel costs.

What deliverables do I receive from OSI?

Under OSI's Patch Management program, OSI searches for and reviews security patches developed by your selected third party/OEM software providers and defines their applicability to the **monarch** software. OSI certifies whether applicable patches are compatible with OSI's **monarch** software products or whether they will cause OSI's **monarch** software products to break down or fail to function properly. OSI will then notify you via a web portal and/or email,

consistent with the frequency of updates associated with your level of Patch Management Service. This notification is in the form of a scheduled report or newsletter.

All patches included in the provided report are considered applicable to OSI systems for security and stability purposes and should be installed or mitigated. OSI's certification report does not list available patches that do not have a security component or consideration. OSI reviews all available updates for each entitlement and excludes patches that are not necessary for meeting NERC-CIP compliance requirements.

We will also provide help desk support to answer any questions you have or to investigate any particular issue up to your maximum incident levels designated for your service level. Optionally we will provide installation services should you require this.

What is not included?

For liability reasons, our services do not include certifying, testing or the offering of any guarantees that the OEM patch itself will fix the offending security problem or that the OEM patch will work as advertised by the OEM. We may, however, share any pertinent experiences with you that we may obtain from working with the OEM patch on our test systems at OSI on an "as is" basis.

How can I contact the PMS help desk?

You can contact the PMS Help Desk coordinator via pms@osii.com or via phone at 763-551-0559.

What are OSI's standard hours of operation for Help Desk Support?

Standard business hours are 8:00 a.m. to 5:00 p.m. Central Standard Time, Monday through Friday, excluding OSI holidays.

What are OSI's holidays?

OSI is closed on the following holidays. On these non-business days, our PMS Help Desk is not available.

- New Year's Day (January 1)
- Memorial Day (Last Monday in May)
- Independence Day (July 4)
- Labor Day (1st Monday of September)
- Thanksgiving Day – United States (4th Thursday in November)
- The Friday following Thanksgiving Day
- Christmas Day (December 25)

How do I know when my PMS plan needs to be renewed?

OSI will contact you prior to the expiration of the system warranty or the current **monarch** PMS program. At this time, an OSI representative will assist you in evaluating your current level of **monarch** PMS and in choosing the plan that best suits your system.

How do I register for monarch PMS?

First, you request a quotation by contacting our Customer Relations group at CustomerRelations@osii.com or quote@osii.com. Next, you accept the quotation and scope of services by sending a purchase order to OSI. Upon receipt of a purchase order for a **monarch** PMS program, OSI will register you with OSI PMS group. The PMS agreement needs to be executed between both parties. A PMS support code will be provided which is tied to your support contract and will change at renewal. You can designate up to three representatives from your company to serve as PMS support coordinators. In order to resolve your PMS support issues quickly and effectively, OSI requests that all PMS support incidents originate with your designated support coordinators.

What if I request services beyond the scope of my plan?

Other services not included in the usual scope of coverage can be quoted as needed on a time and material basis. You can contact your Customer Relations Representative at quote@osii.com for more information.

What happens if I change operating systems or third party products during my service contract?

Any planned major OEM release upgrade (non-security or non-maintenance) must be reported to OSI. Most changes and upgrades made to registered operating systems or third party products are transferable and will be honored. An agreement registration and cost addendum may be required for non-comparable or unsupported products and releases.

How does OSI determine if a security patch is applicable to the monarch software?

A security patch is determined to be applicable if the patch impacts critical product components used by the core OSI software.

Are non-security patches included in the scope of OSI's Patch Management Service?

OSI's Patch Management Service is focused on the management of security patches. However, many non-security patches may be included in a certification effort if the third-party vendor has packaged multiple patches into a single Service Pack or Release.

OSI will also test and report on non-security updates if they are released to complement security updates and/or correct issues caused by defects in security patches.

If I am on the Gold PMS Program (monthly notification) and curious about the status of a newly-released OEM patch, can I receive a status update before the scheduled monthly notification?

OSI recommends that the Patch Management Service you purchase be consistent with your internal Patch Management Policy. If you find that you frequently require expedited updates, you may need to re-evaluate and upgrade your current service level.

What level are the majority of OSI's Patch Management Service customers signed up for?

The current majority of OSI's Patch Management Service customers are on the Gold service level.

Can OSI provide the OEM patches?

Generally, OSI cannot provide you OEM patches. The majority of vendors require you to obtain patches directly through their standard support path.

How does OSI determine which patches are certified since the releases occur at various times during the month?

OSI conducts certification testing during the last week of each month. Any patches released between the 1st of the month to the 21st are included in our testing.

On occasion, OSI may conduct "out-of-band" (off schedule) testing on certain critical patches if determined to be applicable and risk a severe impact on OSI systems. This will be done in order to attempt to certify the critical patches for early deployment on customer environments. Customers will be notified via an announcement on the PMS Web portal if and when this takes place.

Getting in touch with OSI - Other Subjects

OSI welcomes your input about all aspects of our product and service offerings. You may find the following email addresses useful:

- support@osii.com – Customer Support Department
- quote@osii.com– Request sales or product information
- ideas@osii.com – Suggestions for improving products and services
- training@osii.com– **monarch** training information
- sales@osii.com– General questions or information
- CustomerRelations@osii.com – Customer Relations contacts (any subject of interest)