THIRD AMENDMENT TO
PROFESSIONAL VENDOR SERVICES AGREEMENT

OPEN SYSTEMS INTERNATIONAL, INC.

(2013 SCADA System Upgrade Project)

THIS THIRD AMENDMENT TO PROFESSIONAL VENDOR SERVICES AGREEMENT ("Third Amendment") is made and entered into this _____ day of _____, 2017, by and between the CITY OF RIVERSIDE, a California charter city and municipal corporation ("City"), and OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation authorized to do business in California ("Vendor"), with respect to the following facts:

RECITALS

WHEREAS, on or about August 6, 2013, City and Vendor entered into a Professional Vendor Services Agreement for the 2013 SCADA System Upgrade Project ("Agreement"); and

WHEREAS, on or about July 18, 2016, City and Vendor entered into a First Amendment to Professional Vendor Services Agreement for the 2013 SCADA System Upgrade Project; and

WHEREAS, on or about December 13, 2016, City and Vendor entered into a Second Amendment to Professional Vendor Services Agreement for the 2013 SCADA System Upgrade Project; and

WHEREAS, City has identified additional software support and patch management services needed to support the project and desires to amend the Scope and Services of the Agreement to include said services.

NOW, THEREFORE, in consideration of the foregoing recitals which are incorporated herein by this reference, City and Vendor agree as follows:

1. Section 1, "Scope of Services" is hereby amended by adding the additional services identified in Exhibit A-3, attached hereto and incorporated herein by this reference.

2. Section 2, "Compensation/Payment" is hereby amended by adding $698,073 for the additional services, as further identified in Exhibit B-2.

3. All terms and conditions of the Agreement not inconsistent with this Third Amendment, shall remain in full force and effect and are incorporated herein by this reference as if set forth in full.

[Signatures on Next Page]

IN WITNESS WHEREOF, City and Vendor have caused this Third Amendment to Professional Vendor Services Agreement for the 2013 SCADA System Upgrade Project to be duly executed on the day and year first above written.

CITY OF RIVERSIDE, a California charter city and municipal corporation

By: _____
City Manager

Attest: _____
City Clerk

APPROVED AS TO FORM:

By: _____
Assistant City Attorney

OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation authorized to do business in California

By: _____

Ronald Ingram VP
[Name and Title]

By: _____

Bahman Hoveida, President + CEO
[Name and Title]

CA #13-1077.3 SW 12/05/16
Cycom\Wpdocs\D005\P024\00303045.Doc

EXHIBIT A-3

Scope of Services

Professional Vendor Services Agreement

between

The City of Riverside

and

Open Systems International, Inc.

2013

PROFESSIONAL VENDOR SERVICES AGREEMENT

OPEN SYSTEMS INTERNATIONAL, INC.

(2013 SCADA System Upgrade Project)

THIS PROFESSIONAL VENDOR SERVICES AGREEMENT ("Agreement") is made and entered into this 6th day of August, 2013 ("Effective Date"), by and between the CITY OF RIVERSIDE ("City"), a California charter city and municipal corporation, and OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation authorized to do business in California ("Vendor").

1. **Scope of Services**. City agrees to retain and does hereby retain Vendor and Vendor agrees to provide the services more particularly described in Exhibit "A", "Statement of Work" ("SOW"), attached hereto and incorporated herein by reference, in conjunction with 2013 SCADA System Upgrade ("Project").

2. **Term**. This Agreement shall be effective on the date first written above and shall remain in effect until June 30, 2015, unless otherwise terminated pursuant to the provisions herein.

3. **Compensation/Payment**. Vendor shall perform the Services under this Agreement for the total sum not to exceed Seven Hundred Eighty Five Thousand Three Hundred Seven Dollars ($785,307.00) payable in accordance with the terms set forth in Exhibit "A". Said payment shall be made in accordance with the terms set forth in Exhibit "A". 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	To Vendor
Riverside Public Utilities Department Attn: Thanh-Binh Nguyen 2911 Adams Street Riverside, CA 92504	Open Systems International, Inc. Attn: Ken Hall 4101 Arrowhead Drive Medina, MN 55340

5. **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.

(Signatures on Following Page)

IN WITNESS WHEREOF, City and Vendor 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

Approved as to Form:

By: _____
Deputy City Attorney

OPEN SYSTEMS INTERNATIONAL, INC., a Minnesota corporation

By: _____

Name: Bahman Hoveida
President and CEO

By: _____

Name: Ronald Ingram
Secretary

CA#13-1077 sw 06/13/13
O:\Cycom\WPDocs\D013\P016\00162026.docx

EXHIBIT "A"

STATEMENT OF WORK

For

2013 SCADA SYSTEM UPGRADE PROJECT

Appendix D – Price Form

Software Support and Patch Management Option Pricing

Software Support

#	Description	Year1	Year 2 *	Year 3 *	Year 4	Year 5 *	Year 6 *
1	Annual Post-Warranty Software Support (OSI software only, **Gold** level support)	$79,353	$81,734	$84,186	$86,711	$89,313	$91,992
2	Annual Post-Warranty Software Support (OSI software only, **Gold+** level support)	$103,159	$106,254	$109,441	$112,725	$116,106	$119,589
3	Annual Post-Warranty Software Support (OSI software only, **Platinum** level support)	$104,280	$107,408	$110,631	$113,950	$117,368	$120,889
4	Annual Post-Warranty Software Support (OSI software only, **Platinum+** level support)	$130,350	$134,261	$138,288	$142,437	$146,710	$151,111
5	Annual Post-Warranty Software Support (OSI software only, **Diamond** level support)	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses

* Years 2-6 are subject to an escalation of 3% or CPI Index (whichever is higher), for the same scope of services.

Patch Management

#	Description	Year1	Year 2 *	Year 3 *	Year 4	Year 5 *	Year 6 *
1	Annual Patch Management (Post-Warranty, **Gold** level service)	$28,567	$29,424	$30,307	$31,216	$32,153	$33,117
2	Annual Patch Management (Post-Warranty, **Platinum** level service)	$37,137	$38,251	$39,399	$40,581	$41,798	$43,052

* Years 2-6 are subject to an escalation of 3% or CPI Index (whichever is higher), for the same scope of services.

Appendix H – OSI monarch Software Support Plan Overview

monarch™ Software Support Plan Overview

Revision 6.3

September 2012

OSI-555-103-MRK

Table of Contents

1 Overview 1

2 monarch Software Support Components 3

2.1 Maintenance/Problem Fixes 3

2.2 Business Day Support 3

2.3 After-Hours Support 3

2.4 Help Desk 3

2.5 Web-based Training 4

2.6 Software Updates/Subscription 4

2.7 Unlimited Support Incidents 4

2.8 Onsite Installation Assistance 4

2.9 Software Self-Upgrade Assurance 5

3 monarch Software Support Programs 7

3.1 Copper Support Program 7

3.2 Bronze Support Program 7

3.3 Silver Support Program 7

3.4 Gold Support Program 7

3.4.1 Gold Plus Support Program 7

3.5 Platinum Support Program 8

3.5.1 Platinum Plus Support Program 8

3.6 Diamond Support Program 8

4 System Sizing and Complexity: Definitions 11

5 Frequently Asked Questions 13

1 Overview

This document describes the features of the Open Systems International, Inc. (OSI) customer support program for **monarch** software products. OSI has a comprehensive and flexible set of support components to meet various customer needs. General features of the support program include:

- Dedicated department and support staff for handling incoming support calls
- After-hours on-call support service
- 24 x 7 support coverage
- Web-based Customer Support tool
- Web-based supplemental training program
- Fast response for critical support requests
- Comprehensive database tracking and reporting on support incidents
- Software update assurance program
- Tiered pricing based on system size and functionality

The following sections describe the OSI **monarch** software support programs in more detail. 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 and the individual support components selected. Upon request, OSI will quote support services that are not described in this document as part of a customized support plan.

2 monarch Software Support Components

Nine (9) standard components or building blocks make up the various distinct **monarch** software support programs. These components are described below.

2.1 Maintenance/Problem Fixes

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

2.2 Business Day Support

This component allows you to call OSI during business hours for assistance with resolving critical problems with software operation. This is limited to the maximum number of incidents allowed by your plan. *This is comparable to help desk for emergency service requests in dealing with software issues encountered during normal office hours (8 x 5).*

2.3 After-Hours Support

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 plan. *This is comparable to help desk for emergency service requests in dealing with software issues encountered after normal office hours (24 x 7).*

2.4 Help Desk

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 plan. *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 "Engineering Services" program, general consultation services for implementation of projects, engineering of new functions or engineering of new applications, 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 our Customer Relations group to obtain an Engineering Services quotation.

2.5 Web-based Training

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 to our Help Desk 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.

2.6 Software Updates/Subscription

This is a software update subscription or software assurance service that provides you with software updates free of relicensing charges. Normally, this subscription entitles you to receive the pertinent software updates to your licensed software once per annum. (Software releases are made available to you electronically).

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

2.7 Unlimited Support Incidents

This option allows you to uplift your support plan to an unlimited number of Help Desk, Business Day Support and After-Hours Support incidents.

2.8 Onsite Installation Assistance

The Software Assurance/Update 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 will provide the engineering services to perform the upgrade on-site.

OSI personnel will install software upgrades on-site (upon your request), check and certify the new software release with your database and custom features prior to site installation 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 wish to minimize internal budget review and approval processes and roll the cost of such services into a single budgeted annual support fee.

2.9 Software Self-Upgrade Assurance

It is our experience that a majority of the software upgrades performed by our customers ("self-upgrades") result in a much higher number of incidents and unplanned system downtime than upgrades performed by trained OSI personnel. Upgrades, by nature, are more complex than routine system maintenance tasks which customers have been trained to accomplish. As systems grow in complexity and demands for reliability increase, risks associated with self-upgrades also increase. You should consider the following factors when investigating a self-upgrade:

- Risk management
- Project management
- Cost of time and material support for self-upgrade-related incidents
- Expertise and availability of personnel

OSI, by far, offers one of the most competitive software assurance and evergreen update support programs in the industry. It is unheard of and unimaginable for any customer to perform their own upgrades on any of our competitors' systems. Upgrades on these systems are highly complex and are 9-24 month efforts, typically costing nearly the same as the original system or a large fraction thereof. We are committed to offering the best support and upgrade program in the industry while remaining very price competitive. Instead of prohibiting or abolishing self-upgrades, we hope that by offering these added programs we can serve our customers better and raise the quality of their support experiences with OSI.

Those customers wishing to have peace of mind while performing self-upgrades and knowing that their self-inflicted incidents would be handled by OSI outside the normal incident counts must subscribe to this Assurance program via a premium support plan (Support Plus program) as defined in Section 3.

It is important to note that major system upgrades or migrations involving replacement of operating systems or relational databases (for example, UNIX® to Linux®, Oracle® to MySQL™), or upgrading to a much newer release of an operating system (for example, Windows® XP to Vista) should never be attempted as a self-upgrade. This is strongly discouraged and will not be sanctioned by OSI. The complexities of these projects require specific technical knowledge, careful planning, superb project management and execution, and extensive Quality Assurance testing. The impact and risk to the system could be immense.

Software self-upgrades are only allowed under the Premium support plans (Support Plus), and under no circumstances will major upgrades involving wholesale replacement of hardware, operating systems or relational databases be allowed to be attempted by the customer without OSI-sanctioned engineering services assistance.

3 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 1, to devise a customized and cost-effective support plan for customers with various needs or budgets.

3.1 Copper Support Program

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

3.2 Bronze Support Program

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

3.3 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 plan does **not** include after-hours support service **nor** does it entitle you to receive new releases of licensed OSI software.

3.4 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 and OSI's wiki-based online documentation site, **OSI-PEDIA**. Included in this plan 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 plan and can be purchased separately. OSI will quote engineering services for an upgrade plan tailored to your specific needs.

3.4.1 Gold Plus Support Program

Those customers who would want to perform their own upgrade installations (self-upgrade) are required to subscribe to the Gold or Platinum Plus Software Support program. Gold Plus includes all features in the Gold plan plus an assurance program for OSI to provide support for incidents resulting from a self-upgrade process.

OSI will track and address these incidents separately from the normal incidents typically submitted on an operational system and will guarantee top priority handling of these incidents. These incidents are typically self-inflicted incidents. They result from improper planning or lack of adequate knowledge for engineering systems and may not be inherent software problems. This plan provides an assurance that OSI is standing by in case there are issues to be elevated to OSI to assist with. This plan is not an engineering services plan to assist with the upgrade nor does it provide the customer with additional labor or documentation for performing the upgrade. OSI requires that activities be coordinated with the Support department to ensure better handling of issues.

3.5 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 and OSI's wiki-based online documentation site, **OSI-PEDIA**. Included in this plan are new releases of the applicable licensed OSI software (in electronic format) for your system. Installation services are not included as part of this plan and can be purchased separately. OSI will quote engineering services for an upgrade plan tailored to your specific needs.

3.5.1 Platinum Plus Support Program

The Platinum Plus support program allows customers who are on a Platinum support plan to receive an assurance program for handling incidents resulting from a software upgrade performed by the customer and without OSI engineering assistance.

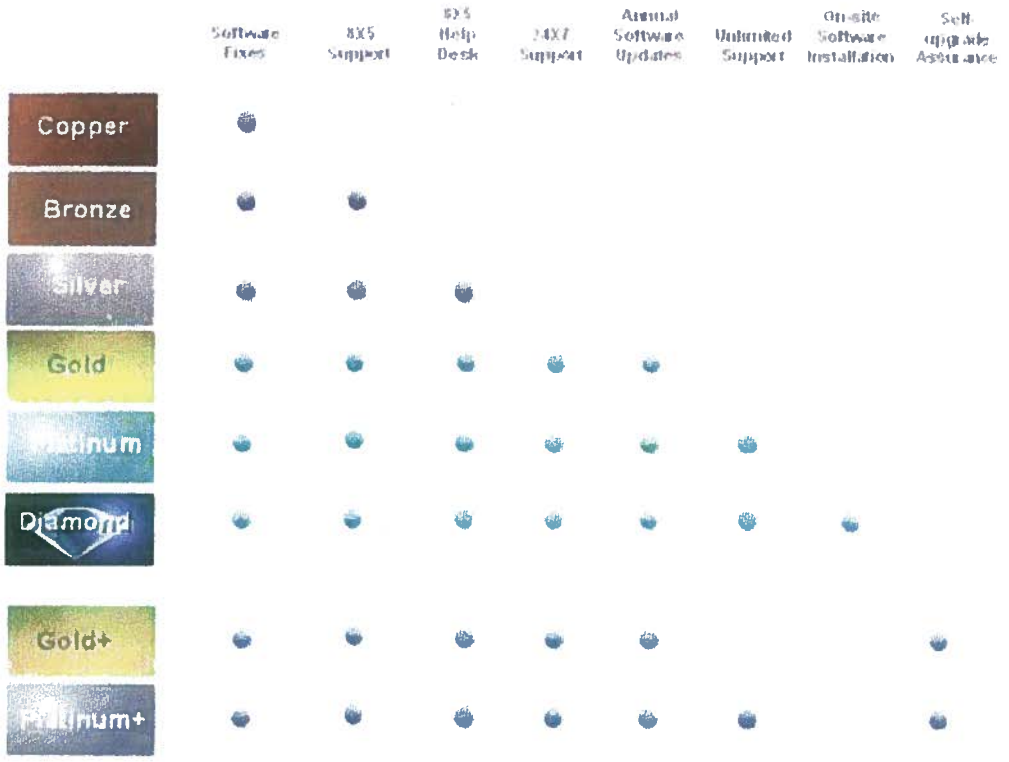
OSI will track and address these incidents separately from the normal incidents typically submitted on an operational system and will guarantee top priority handling of these incidents. These incidents are typically self-inflicted incidents. They result from improper planning or lack of adequate knowledge for engineering systems and are not inherent software problems. This plan provides an assurance that OSI is standing by in case there are issues to be elevated to OSI to assist with. This plan is not an engineering services plan to assist with the upgrade nor does it provide the customer with additional labor or documentation for performing the upgrade. OSI requires that activities be coordinated with the Support department to ensure better handling of issues.

3.6 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 and OSI's wiki-based online documentation site, **OSI-PEDIA**. Included in this plan are new releases of the applicable licensed OSI software along with on-site installation assistance once per year. Note: This includes the engineering time to install the new releases but 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.

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



Web-based training sessions and **OSI-PEDIA** are a standard feature of all Premium support plans (Gold level and greater) and are included free of charge with these plans.

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

4 System Sizing and Complexity: Definitions

In order to provide fair tiered pricing for the support plans, the plans are graduated for various system sizes in terms of number of Remote Terminal Units (RTUs) and/or database point sizes into the following categories. (Contractual maximum sizing is used for these calculations.)

- **Mini** 20 RTUs and <1,000 points
- **Small** 0-49 RTUs and 1,000-4,999 points
- **Medium** 50-99 RTUs and 5,000-9,999 points
- **Large** 00-199 RTUs and 10,000-24,999 points
- **X-Large** 200-399 RTUs and 25,000-49,999 points
- **Jumbo** 400 RTUs and ≥ 50,000 points

The following cost multipliers for specific system characteristics 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 Center
- Specials and Custom Applications
- Program Development Systems

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

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. 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 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 plan needs to be renewed?

For customers exiting warranty, OSI will contact you prior to the expiration of the system warranty. 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 plan that best suits your system.

How do I register for OSI Support?

Upon receipt of a purchase order for a **monarch** software support program, OSI will register you with OSI Customer Support. A 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 support coordinators. In order to resolve your support issues quickly and effectively, OSI requires that all support incidents are only submitted by your designated support coordinators.

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

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 our customers are qualified and well trained in OSI's software and platform technology. We also highly recommend that they keep their training refreshed in subsequent years.

You can designate up to three (3) 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.

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.

How are Incidents Defined?

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:

Critical incidents are those that inhibit essential software operation and/or result in a substantial loss of operational capability. Critical software problems as an example 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, an on-call engineer will return your call promptly (generally within 30 minutes).

Non-Critical Incidents:

Non-critical incidents include any problems or questions related to system functionality that do not disrupt essential operations. For example, minor software problems, non-disruptive errors in user interface and displays, errors in documentation, questions related to how program functions work, help desk support and similar issues. OSI guarantees a 24-hour response (Monday through Friday) on all non-critical help requests and questions. Depending on the availability of our on-call engineers, most requests will be handled within the same business day.

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 were not designed to be a general services program to provide assistance and consulting for 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 engineering services beyond ordinary support are required. The OSI standard support organization is not 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 engineering services.

What should I do if I need support?

When an incident arises, your 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 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 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 recommend that you request support for critical 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 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 Incident 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 plan?

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 plans.

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 Plan?

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 15% to 20% 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 cost justifications for enrolling in the support program and how can I convince my management to purchase support?

There are three 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

- Improvements and enhancements are received with software updates, which defers future repurchases of software licenses

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 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 plans minimize the level of additional internal support staffing that is otherwise needed.

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

Software upgrades have an intrinsic value because your software investment does not become obsolete as time passes and technology changes. Assuming a 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 plans?

Yes! There are discounts available for multiple-year commitments that are paid in full at the onset of the support plan. 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 customerrelatiotions@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 and many other consulting needs. Please contact your Customer Relations representative at customerrelations@osii.com for additional information.

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 and **OSI University** information
- sales@osii.com - General questions or information regarding new project needs
- customerrelations@osii.com - Customer Relations for general assistance

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.

Appendix I – OSI monarch Patch Management Service Plan Overview

monarch™ Patch Management Service Plan Overview

Revision 1.3
January 2008
OSI-555-105-MRK

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

3 Optional Services 9
- 3.1 Remote Patch Installation 9
- 3.2 On-Site Patch Installation 9
- 3.3 System Audit 9

4 monarch PMS Programs 11
- 4.1 Silver PMS Program 11
- 4.2 Gold PMS Program 11
- 4.3 Platinum PMS Program 11

5 Deploying a Successful Patch Management Strategy 13

6 PMS: Legal Disclaimer 15

7 Sample PMS Agreement 17

8 Frequently Asked Questions 21

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 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 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.

- 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, 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.

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 time frame consistent with the level of service to which you have subscribed) of the applicability and compatibility definition 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. 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 login name to navigate to the Patch Management 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 on topics regarding patch installation and verification. The sessions are designed to provide in-depth and topic-specific training in a small group setting. Courses are open to enrollment on a first-come, first-served basis. This training session provides instruction on how to install patches and audit systems as well as other PMS topics of interest and PMS best practices.

3 Optional Services

Additional optional services can be provided on a time and materials basis to assist you with your Patch Management activities.

3.1 Remote Patch Installation

Customers that provide remote access can subscribe to a remote patch installation service. Trained OSI staff will install patches (both the OEM patches as well as any applicable or required **monarch** patches) under the supervision of the customer via remote connection on a time and materials basis (at an hourly engineering rate). An audit will be performed at the end of each installation. OSI will provide records for all installations for your auditing and record keeping purposes.

3.2 On-Site Patch Installation

OSI personnel can provide on-site services both for installation and verification of certified patches on a time and material basis.

At the end of the installation, a summary report will be provided for your records.

Registration of each computer requiring patch installation is required prior to travel arrangements (actual travel and living costs associated with the trip will be invoiced separately).

3.3 System Audit

OSI can perform a comprehensive annual audit of your **monarch** system to verify the patch levels and the state of your system relating to OEM patches. This service can be provided remotely or onsite, depending on your preference, on a time and material basis.

4 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.

Patch Management service levels offered are:

- Silver PMS service
- Gold PMS service
- Platinum PMS service

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

4.1 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.

4.2 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.

4.3 Platinum PMS Program

The Platinum PMS Program is our premium service plan and includes **weekly** analysis and certification of **monarch** software for registered third-party/OEM software Platinum program provides for help desk support for up to **80** 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.

5 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 ways to go about 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 getting the latest and greatest patch 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 viruses to deal with, such as "Mydoom," "Nimda" and "Slammer" - which ironically had a patch available two full years before wreaking havoc on businesses throughout the world in 2004. There does not appear to be any sign of a slowdown. Microsoft issued 12 security bulletins covering 17 patches in a single month alone in 2005! 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.

6 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. 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.

For full legal disclosure, please refer to Section 7 for a sample PMS contract.

7 Sample PMS Agreement

Agreement for Patch Management Services

This Agreement For Patch Management Services ["Contract"] is between Open Systems International, Inc. [hereafter "OSI"] and _____ [hereafter "Customer"] and shall apply to the Work described in the attached Schedules and any related and attached Purchase Orders unless specifically modified in writing and agreed to between the Parties. This Contract shall be effective beginning _____, 200_

1. **Services Provided:** OSI's Patch Management Services are intended to facilitate and assist Customer in the tracking of third-party security patches, determination of their applicability to **monarch** software, and assessment of the potential impact of the patch on **monarch** software. OSI's patch management services will assist Customer in the following areas:

   - **Applicability:** OSI will determine and evaluate the applicability of the OEM patch in relation to the core functionality of the **monarch** software, answering the question: Yes, the patch is applicable; or no, the patch is not applicable to Customer's **monarch** software.
   - **Compatibility:** OSI will determine whether an applicable 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 Customer's **monarch** software or impact the **monarch** system operation, Customer will be advised to abstain from installing it until a corresponding compatible **monarch** patch is available from OSI. For offending OEM patches which are critical to Customer's system, OSI will provide workarounds or an OSI software patch to make sure the operation of Customer's **monarch** system after the patch installation remains unchanged.
   - **Help Desk:** OSI will provide a Help and Support Desk to answer any questions on Customer's patch installation of the OSI patches.
   - **Other Support:** Optionally OSI can provide Customer with engineering services and labor to install the OEM patch as well as the OSI patch, either through remote support or in some cases via on-site services.

2. **Services Not Provided:** OSI's services do not include certifying, testing, or offering 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. OSI may, however, share any pertinent experiences with Customer which we may obtain from working with the OEM patch on our test systems at OSI on an "as is" basis without any warranty as to the accuracy or completeness of such information or its applicability to Customer's system.

3. **Deliverables under OSI's Patch Management Service:** Under OSI's Patch Management program, OSI searches for and reviews security patches developed by Customer-chosen 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 Customer via a web portal and/or email, consistent with the frequency of updates associated with Customer's level of Patch Management Service. OSI will also provide help desk support to answer any questions Customer may have or to investigate any particular issue up to Customer's maximum incident levels designated for Customer's service level. Optionally, OSI will provide installation services should Customer require these services.

4. **Warranty and Limitation of Liability:** OSI's service and certification is limited to a determination of whether the applicable 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 software patch is necessary for or applicable to Customer's specific system configuration, includes any defects or vulnerabilities, or will enhance the security, performance or reliability of Customer's system.

   OSI will use its best efforts to determine and certify the compatibility of the patches discovered with OSI's **monarch** software products, in a professional manner and based upon the industry's best practices. 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 Customer on a timely basis if and when the compatibility can be provided. Neither OSI's liability nor Customer's available remedies shall be increased by the patch management services offered, beyond that specified in Customer's OSI Software License Agreement or Support Services Agreement.

5. **Payment Terms:** The amount and schedule of payments shall be as stated on the attached Schedule A.

6. **Level of Service:** As explained in detail on the attached Schedule B, OSI offers the following Patch Management service levels:

   - Silver service
   - Gold service
   - Platinum service

   Based on the service plan that is selected, subscribers will then be notified of certified patches at varying frequencies such as quarterly, monthly, or weekly/immediately upon availability.

   Customer's contracted service level is stated on the attached Schedule A.

7. **Prerequisites to Enrollment in the Patch Management Service:** In order to subscribe to OSI's Patch Management Service, Customer must be enrolled in a **monarch** Gold Warranty, or a Gold, Platinum or Diamond support plan. Customer's enrollment in an active support plan provides the basis for Customer to be able to receive OSI software updates (and patches to OSI software) if needed. If Customer is not enrolled in a premium **monarch** support plan and wishes to subscribe to the OSI Patch Management Service, Customer must first subscribe to an OSI Gold, Platinum or Diamond support plan.

8. **Termination:** Either party may terminate this Contract with or without cause upon 60 days written notice.

9. **No Assignment:** Neither Party may assign or transfer its interest in this Contract without the prior written consent of the other Party.

10. **Ownership of Work Product/Intellectual Property Rights:** This Contract is not intended to establish, transfer or alter the intellectual property rights of either Party to the other Party and all designs and development shall be considered the work product of its creator or designer.

11. **Confidentiality:** Each Party agrees that should information which is proprietary or confidential (hereinafter "Confidential Information"), as designated and marked by the Party providing the information ("Disclosing Party"), be shared with the other Party, ("Receiving Party") the Receiving Party shall not disclose this Confidential Information to anyone or use this Confidential Information for any purpose independent of the efforts and purposes of this Contract. Any Party receiving Confidential Information shall use such Confidential Information only for the benefit of both Parties as intended in connection with this Contract 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. Each 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. This Section 11 shall survive the termination of this Contract.

    In the event either Party receives a subpoena or other validly issued administrative or judicial process demanding Confidential Information of the other Party, the Receiving Party shall promptly notify the Disclosing Party and tender to it the defense of such demand. Unless the demand shall have been timely limited, quashed or extended, the Receiving Party shall thereafter be entitled to comply with such demand to the extent permitted by law. If requested by the Party to whom the defense has been tendered, the Receiving Party shall cooperate (at the expense of the Disclosing Party) in the defense of a demand.

12. **Dispute Resolution:** The Parties acknowledge that unauthorized disclosure of Confidential Information or other breach of any obligation under this Contract 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 Contract.

    Any other dispute, for claims which will not result in irreparable harm if not immediately addressed, may be brought for decision in any court of competent jurisdiction only after the parties have met and attempted to amiably resolve the dispute.

13. **Non-Solicitation of Employees**. Each Party agrees that during the term of the Contract, and for a period of one (1) year thereafter, it will not directly or indirectly solicit, hire, or retain for employment or contract services any employee or contractor of the other Party.

    The Parties acknowledge that unauthorized solicitation of the other Party's employees 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 provision.

14. **Notice:** Any Notices to be provided pursuant to this Contract shall be sent to the undersigned at the respective addresses stated below their signatures unless otherwise designated by either Party in writing. Notices shall be provided by commercial courier or certified mail.

15. **Governing Laws** Any action related to the terms set forth in this Contract or interpretation of this Contract will be governed by Minnesota law, excluding choice of law rules.

Agreed to and Accepted by:

OPEN SYSTEMS INTERNATIONAL, INC.

3600 Holly Lane North, Suite 40

Minneapolis, MN 55447-1286

Signature

Date: _____

Agreed to and Accepted by:

Signature

Date: _____

8 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.

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.

For example, there are many components of the Windows XP Professional operating system. OSI tracks and maintains a list of all critical Windows XP Professional components used by the **monarch** software. A Windows XP Professional patch will be defined as applicable if the patch impacts any critical Windows XP Professional components used by the **monarch** software.

Some examples of Windows XP Professional components include: TCP Stack, Media Player, Internet Explorer, Calculator, Hyper Terminal, Remote Desktop and so on.

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.

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 to the Platinum 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.

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)

This page left blank intentionally.

RIVERSIDE PUBLIC UTILITIES

Board Memorandum

BOARD OF PUBLIC UTILITIES **DATE:** August 2, 2013

ITEM NO: 11

SUBJECT: **ELECTRIC SCADA SYSTEM HARDWARE, SOFTWARE, AND NETWORK UPGRADE PROJECT - WORK ORDER NO. 1024305**

ISSUE:

The item for Board of Public Utilities consideration is approval of additional funds in the amount of $2,258,307 for Work Order No. 1024305 for the procurement, installation, configuration, testing and training of the Electric Supervisory Control and Data Acquisition (SCADA) System Software, Hardware and Network Upgrade Project, Phase 2 - Implementation.

RECOMMENDATIONS:

That the Board of Public Utilities:

1. Approve additional capital expenditure of $2,258,307 for Work Order No.1024305 for the procurement, installation, configuration, testing and training of the Electric SCADA System Software, Hardware, and Network Upgrade Project, Phase 2 – Implementation ("Project");
2. Approve the award of SCADA Software Upgrades contract to Open Systems International, Inc. (OSI), the current SCADA vendor, in the amount of $785,307;
3. Authorize the General Manager, or his designee, to amend the OSI Agreement in an amount not-to-exceed 15% in the event that additional services beyond the scope of the Agreement are needed; and
4. Authorize the procurement of Hewlett Packard (HP) servers and workstations and Dell laptops for the Project in an amount not-to-exceed $388,000.

BACKGROUND:

Supervisory Control and Data Acquisition (SCADA) systems are the primary tools to operate, control and obtain data for electric utilities. Riverside Public Utilities' (RPU) SCADA system collects data from various sensors at substations and other control points throughout RPU's grid and sends these data to computer servers which then manages and controls the data. The SCADA system is operated and controlled from the Utilities Operations Center (UOC) Dispatch.

The Board of Public Utilities approved Work Order No. 1024305 on July 1, 2011 for the capital expenditure of $230,000 for the Planning, Engineering, Consulting Services, Training and Travel of the SCADA System Upgrade Project, Phase 1 – Planning. On September 21, 2012, the Board approved additional capital expenditure of $250,000 for KEMA, Inc. for additional consulting services. The approved cost for the first phase of the SCADA Upgrade project encompassing Planning, Engineering, Training, Travel and Consulting Services are broken down as follows:

Approved: Phase 1 – Planning & Engineering		
	Descriptions	**Cost**
1	KEMA, Inc. consulting services	$ 160,050
2	Planning and Engineering	$ 54,950
3	Training and Travel	$ 15,000
	(July 1, 2011) **Sub-Total:**	**$ 230,000**
4	KEMA, Inc. additional consulting services	$ 250,000
	(September 21, 2012) **Accumulative Total:**	**$ 480,000**

With Phase 1 - Planning concluding, the next stage of the SCADA Upgrade Project, Phase 2 - Implementation is now ready to be initiated. Phase 2 - Implementation is divided into three parts for clarity and ease of project management and coordination. The three parts consist of Software Upgrade, Hardware Upgrade, and Network Upgrade & Re-Configuration.

For the Software Upgrade, staff recommends that OSI continues to be RPU's SCADA vendor as it will be in the City's best interest. Through lengthy negotiations, OSI and RPU have come to an agreement on the most suitable scope of work for the City and at the best possible price. The SCADA Software Upgrade with OSI will not only provide continuity of service and maintain RPU personnel's familiarity to the SCADA platform but also the following:

1. Deliver critical fundamental upgrades to the SCADA System not realized since 2007;
2. Enable new powerful features and content to SCADA users and system administrators;
3. Position the City to meet evolving North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements applicable to Distribution Providers. (*NERC is the electric reliability organization certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce reliability standards for the bulk power system.*)

The Professional Vendor Services Agreement contains certain information that describes or otherwise depicts the City's SCADA system. In order to protect the integrity and safety of the SCADA system, this information has been redacted from the publicly viewable version of this agreement.

For the Hardware Upgrade, staff recommends that all SCADA hardware, including servers, workstations, laptops, system backup tape machines, server racks monitors/switches/cables, and all required peripherals be replaced to facilitate the Software Upgrade scope of work. Computing devices such as those listed above generally have a life expectancy of three to five years. The life expectancy is contributable not only to regular wear and tear, but also to technological advances as well as greater data processing, memory, and speed requirements for new applications and their version updates. RPU staff plans to purchase and configure all SCADA hardware and related operating system software ensuring correct installations and minimizing compatibility issues.

Finally, for the Network Upgrade & Re-Configuration, staff recommends that the SCADA Local Area Network (LAN) be renovated to a more rigorous NERC CIP compliant design. The new re-designed SCADA LAN will resolve current problematic failover issues, reduce LAN traffic, diminish congestion from Backup processes, and increase Network security. Most importantly, it will isolate system functions between firewalls effectively creating quarantine areas, containing viruses and malwares should one be introduced maliciously or inadvertently. The new Wide Area Network (WAN) consisting of independent Synchronous Optical Networking (SONET) links will also be installed between the UOC (Primary site) and Riverside Energy Resource Center (RERC – Backup site) to facilitate the new SCADA LAN communication. RPU staff plans to purchase, install, and configure all SCADA LAN and WAN equipment including switches, firewalls and all required hardware and software for this project.

The cost for the SCADA Upgrade Project Phase 2 – Implementation which includes engineering/planning, procurement, installation, configuration, testing and training are as follows:

Request: Phase 2 – Implementation		
	Descriptions	**Cost**
1	OSI SCADA Software Upgrade and Options	$ 785,307
2	SCADA Hardware Estimate	$ 388,000
3	Network Hardware and Labor Estimate	$ 379,000
4	RPU Labor and Overhead	$ 483,000
5	Training and Travel	$ 25,000
6	Engineering and Planning	$ 80,000
7	Contingencies	$ 118,000
	Total:	**$ 2,258,307**

FISCAL IMPACT:

The total revised SCADA Upgrade Project cost for Phase 2 is estimated at $2,258,307. Sufficient funds are available in the Capital Improvement SCADA Account No. 6130000-470672.

Prepared by:	Stephen H. Badgett, Public Utilities Deputy General Manager
Approved by:	David H. Wright, Public Utilities General Manager
Approved by:	Belinda J. Graham, Assistant City Manager
Approved as to form:	Gregory P. Priamos, City Attorney

Certifies availability of funds:

for Laura Chavez-Nomura
Public Utilities Assistant General Manager
Finance/ Administration

Attachment:
1 Agreement

EXHIBIT B-2

Compensation

Appendix D – Price Form

Software Support and Patch Management Option Pricing

Software Support

#	Description	Year1	Year 2 *	Year 3 *	Year 4	Year 5 *	Year 6 *
1	Annual Post-Warranty Software Support (OSI software only, **Gold** level support)	$79,353	$81,734	$84,186	$86,711	$89,313	$91,992
2	Annual Post-Warranty Software Support (OSI software only, **Gold+** level support)	$103,159	$106,254	$109,441	$112,725	$116,106	$119,589
3	Annual Post-Warranty Software Support (OSI software only, **Platinum** level support)	$104,280	$107,408	$110,631	$113,950	$117,368	$120,889
4	Annual Post-Warranty Software Support (OSI software only, **Platinum+** level support)	$130,350	$134,261	$138,288	$142,437	$146,710	$151,111
5	Annual Post-Warranty Software Support (OSI software only, **Diamond** level support)	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses	Platinum level plus Time & Materials plus travel expenses

* Years 2-6 are subject to an escalation of 3% or CPI Index (whichever is higher), for the same scope of services.

Patch Management

#	Description	Year1	Year 2 *	Year 3 *	Year 4	Year 5 *	Year 6 *
1	Annual Patch Management (Post-Warranty, **Gold** level service)	$28,567	$29,424	$30,307	$31,216	$32,153	$33,117
2	Annual Patch Management (Post-Warranty, **Platinum** level service)	$37,137	$38,251	$39,399	$40,581	$41,798	$43,052

* Years 2-6 are subject to an escalation of 3% or CPI Index (whichever is higher), for the same scope of services.