RIVERSIDE PUBLIC UTILITIES

Board Memorandum

BOARD OF PUBLIC UTILITIES **DATE: FEBRUARY 24, 2025**

SUBJECT: REQUEST FOR PROPOSAL NO. 2340 - PROFESSIONAL CONSULTING SERVICES AGREEMENT WITH AESI, INC. FOR CYBER SECURITY FOR A THREE-YEAR TERM, IN THE AMOUNT OF $329,100

ISSUE:

Consider recommending that the City Council approve a Professional Consultant Services Agreement with AESI-US (AESI), Inc. for cybersecurity consulting services from Request for Proposal No. 2340 for a three-year term, in the amount of $329,100, to include items such as a cyber program assessment, cyber posture assessment, vulnerability assessment services, penetration testing services, remediation services, incident response services, training services, mentoring services, and exercise services.

RECOMMENDATIONS:

That the Board of Public Utilities recommend that the City Council:

1. Approve the Professional Consultant Services Agreement with AESI-US, Inc., from RFP No. 2340 for cybersecurity consulting services, for a three-year term, in an amount of $329,100; and

2. Authorize the City Manager, or his designee, to execute the agreements, including making minor non-substantive changes, and to sign all documents and instruments necessary to complete the transactions.

REGULATORY HISTORY:

The history surrounding North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)-008 and NERC CIP-013 reflects an evolving regulatory landscape aimed at reinforcing the cybersecurity posture of the North American bulk power system. NERC CIP-008, which addresses incident reporting and response planning, has its roots in earlier versions of the CIP standards established in response to increasing cyber threats to the energy sector. Over time, these standards have been refined to require more rigorous and detailed incident management processes, reflecting the growing recognition of cyber threats as a significant risk to grid reliability. Similarly, NERC CIP-013, which focuses on supply chain risk management, was introduced as a direct response to vulnerabilities identified in the supply chain of critical infrastructure components. The standard mandates that utilities implement comprehensive risk management plans for their supply chains, including vendor security controls and continuous monitoring. Given

the complexity and technical specificity of these standards, as well as the need for compliance with evolving regulatory expectations, it is prudent for RPU to retain a specialized cybersecurity consultant. A cybersecurity consultant can provide expert guidance in navigating these legislative requirements, ensuring that the utility's cybersecurity practices not only comply with current standards but also proactively address emerging threats.

BACKGROUND:

The ability to provide and support comprehensive cyber security protection across Riverside Public Utilities (RPU) is essential for maintaining a secure and robust cyber environment. The rapid and ever-changing threat landscape in the utility sector can only be mitigated if RPU utilizes every resource available to keep its Operational Technology (OT) systems and environments at a maximum protection level.

It was crucial that RPU develop a Cyber Security Professional Consulting Services Request for Proposal (RFP) to continue to enhance our security posture. This RFP sought a qualified vendor to perform a comprehensive review of RPU OT network architecture, security controls, policies, facilities, and systems to identify gaps in and provide mitigation solutions for Critical Infrastructure Protection.

The cyber security services requested in RFP 2340 requires an approach that is both modular and capable of maintenance by RPU personnel. This effort is to ensure that the Utility maintains a strong and consistent cybersecurity posture. The initial scope of services for this project will include a comprehensive Cyber Program Assessment followed by a Cyber Posture Assessment.

DISCUSSION:

On May 8, 2024, City staff posted RFP No. 2340 on the City's online bidding system, Planet Bids seeking Cyber Security Professional Consulting Services. Proposers were requested to submit proposals for a complete solution only. The RFP actions are summarized in the following table:

Action	Number
External Vendors Notified	500
City of Riverside Vendors	308
Prospective Bidders Who Downloaded the RFP	83
Questions and Answers Submitted	64
Non-Mandatory Virtual Meeting	1
Non-Responsive Proposals Received	1
Responsive Proposals Received	8

RFP No. 2340 closed on June 12, 2024, with nine proposals. After the Purchasing division reviewed all submitted proposals, one proposal was deemed non-responsive due to incomplete submission of documentation.

Under the guidance of the Purchasing Division, four City staff members evaluated the proposals based on the following selection criteria:

A. Qualifications (35%)

B. Pricing (20%)
C. Experience (Projects of similar size and scope) (25%)
D. Approach and Methodology (10%)
E. Professional References (10%)

The evaluation ranking results are shown in Table 1. Additionally, Table 2 shows the scores for the four technical criteria used to judge each proposal, in addition to the vendor's cost proposal. (The sum of the technical scores had a maximum possible weight of 80% and the cost proposal had an additional 20% weight.) Four panelists scored the technical criterion, while City Purchasing scored the cost proposal.

Table 1. Evaluation Result Ranking

Proposers	Evaluation Ranking Results
AESI-US, Inc	1
Archer Energy Solutions, LLC	2
BayInfotech LLC	3
Net Force	4
Global Solutions Group, Inc.	5
Global Information Intelligence LLC	6
Elegant Enterprise-Wide Solutions, Inc.	7
TAC Security Inc.	8

Table 2. Evaluation Scoring Results

Criteria	AESI-US, Inc	Archer Energy Solutions LLC	BayInfoTech LLC	Net Force	Global Solutions Group Inc.	Global Information Intelligence LLC	Elegant Enterprise-Wide Inc.	TAC Security Inc.
Approach & Methodology (10%)	90%	70%	60%	73%	60%	45%	60%	40%
Experience (25%)	90%	93%	50%	68%	48%	45%	53%	40%
Professional References (10%)	80%	83%	40%	53%	55%	65%	43%	30%
Qualifications (35%)	88%	93%	53%	70%	45%	55%	53%	35%
Technical Score (weighted)	88%	89%	51%	67%	49%	52%	52%	37%
Cost Proposal (20%)	26%	13%	100%	12%	46%	16%	3%	20%
Overall Score	**75%**	**73%**	**61%**	**54%**	**48%**	**45%**	**42%**	**33%**

Eleven (11) items were listed in the Scope with respective bidders submitting their proposals for

1) hourly rate and 2) estimated hours. These items included:

- Cyber Program Assessment
- Cyber Posture Assessment
- Vulnerability Assessment Services
- Penetration Testing Services
- Remediation Services
- Incident Response Services
- In-Person or Virtual Training Services
- One-on-One Mentoring Services
- Laboratory Services
- Budget Scope
- Exercise Services

Cost proposals ranged from below $100,000 to above $1,000,000, with AESI submitting the third lowest cost proposal. The technical scores and cost score were then combined into a final, total overall score. Based on this process, AESI scored the highest with an overall total score of 75% and a superior technical score of 88%.

After the evaluation of the proposals, the evaluation panel selected AESI as the preferred vendor for the cyber security professional services.

Purchasing Resolution 24101 Section 508 states, "Contract procured through Formal Procurement shall be awarded by the Awarding Entity to the Lowest Responsive and Responsible Bidder, except that…(c) Contracts procured through Formal Procurement for Services or Professional Services, where a Request for Proposals or Request for Qualifications was used to solicit Bids, shall be awarded by the Awarding Entity in accordance with the evaluation criteria set forth in the Request for Proposals or Request for Qualifications…"

The Purchasing Manager concurs that the recommended actions comply with the City of Riverside's Purchasing Resolution No. 24101.

The term of the Professional Consultant Services Agreement will be three years with a total possible compensation of $329,100 as shown in Table 3. During this contract, it is possible an adverse event could arise, or cyber incident could occur resulting in immediate decision making and approval. To protect against any delays, the agreement with AESI includes an additional, not-to-exceed option of $50,000 per year, should any unforeseen incidents occur. The inclusion of this contingency option is a precautionary measure that will only be used to address such incidents, should any occur. All hourly rates will be consistent with the quoted rates stated within the proposal. No work will be approved without the explicit approval of the Project Manager.

Table 3. Contracted Amount and Contingency Option Over a 3-Year Period

AESI-US, Inc.	Year 1	Year 2	Year 3	Total
Contracted Amount	$60,000	$60,000	$59,100	$179,100
Contingency Option	$50,000	$50,000	$50,000	$150,000
				$329,100

AESI-US, Inc.

AESI-US, Inc. offers a full spectrum of cyber security services ranging from training, risk assessments, governance, cyber program development, vulnerability assessments, technology integration, and technology implementation and remediation. AESI has completed more than 250 cybersecurity-related projects on utility corporate systems and networks, Supervisory Control and Data Acquisition (SCADA) systems, Advanced Metering Infrastructure (AMI), Distributed Control Systems, and Distributed Energy Resources for over 200 electric and water utilities across North America. They have in depth knowledge of both Information Technology and Operational Technology systems and environments.

Additionally, AESI has worked extensively over the years with Hometown Connections (a non-profit utility services organization), the American Public Power Association (APPA), Joint Action Agencies (JAAs) and Joint Powers Authorities (JPAs). AESI fully understands the size and range of requirements of public power and water utilities and has developed capabilities and packages to meet the requirements of small, mid-sized and large utilities, and JAAs/JPAs.

The Cyber Program Assessment will provide a clear picture of RPU's current overall cyber security strengths and weaknesses, enabling staff to prioritize improvements and build a more resilient security program to increase cyber maturity. Previous assessments have successfully identified areas of strength and vulnerability, leading to the development of targeted action plans that have significantly bolstered RPU's cyber security posture.

Additionally, the program assessment will focus on the following areas:

- OT System Identification and Categorization
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeter
- Physical Security of OT Systems and Facilities
- System Security Management
- Incident Reporting and Response Training – CIP-008
- Recovery Planning for OT Systems
- Configuration Change Management and Vulnerability Assessments
- Information Protection
- Supply Chain Risk Management – CIP-013

RPU will gain a comprehensive, tailored approach to safeguarding its critical infrastructure, and AESI's expertise ensures that new or existing programs are maximized for effectiveness in threat detection and mitigation. RPU's program for continuous monitoring and scanning of tools and processes will also be reviewed as these tools are reintroduced to the OT environment and as SCADA systems are replaced and upgraded.

Recommendations from AESI's Cyber Posture Assessment will be included and incorporated into RPU's Cyber Program Framework. The continued development of a comprehensive risk mitigation plan will address any identified vulnerabilities and outline specific mitigation solutions. This phase may involve conducting detailed vulnerability assessments, including system scans, risk analyses of critical systems, and providing targeted remediation advisement. AESI's external network penetration services in previous engagements have demonstrated the resilience of

access points into the OT environment and the effectiveness of RPU's monitoring and detection systems.

AESI has previously conducted vulnerability assessments for RPU, identifying known vulnerabilities and insecure settings. Additionally, AESI reviewed and analyzed firewall configurations to detect any insecure setups. RPU implemented the recommendations, thereby hardening the OT environment and reducing its cyber security risk. AESI will continue these vulnerability assessment services to help RPU mitigate cyber security threats as new vulnerabilities emerge.

The flexibility of the scope allows staff to incorporate additional services as needed based on the assessment outcomes, ensuring that the approach remains adaptive and responsive to evolving threats. This structured and thorough process aims to significantly enhance RPU's cybersecurity defenses, safeguarding its critical infrastructure and ensuring the resilience of its operations.

In conjunction with ensuring a strong, resilient utility, AESI will provide critical knowledge transfer to RPU employees. This knowledge transfer will be provided through virtual or in-person training and cybersecurity tabletop exercises to ensure a continuous and proactive approach to cybersecurity.

The Chief Innovation Officer concurs with the recommended actions comply with the City of Riverside's Technology and Acquisition Policy.

STRATEGIC PLAN ALIGNMENT:

This item contributes to:

Strategic Priority No. 6 - Infrastructure, Mobility and Connectivity and Goal 6.2 - Maintain, protect, and improve assets and infrastructure within the City's built environment to ensure and enhance reliability, resiliency, sustainability, and facilitate connectivity.

This item also aligns with each of the five Cross-Cutting Threads as follows:

1. **Community Trust** – RPU is committed to the highest quality water and electric services at the lowest possible rates to benefit the community. This procurement helps ensure that we have up-to-date, hardened technology to continue delivering safe and reliable service to RPU customers.
2. **Equity** – The OT infrastructure is critical to the delivery of reliable power and protecting this infrastructure ensures equitable distribution of services to every member of the community.
3. **Fiscal Responsibility** – This procurement has been done under an open RFP process designed to select the most well qualified consultants that supplied fiscally sound and reasonable bids.
4. **Innovation** – This procurement ensures that RPU's most critical electric and water operating and monitoring system is up to date with the most current cybersecurity technology and security settings available.

5. **Sustainability & Resiliency** – This procurement was designed to include continued cyber program and posture assessments to remain current with the industry's best practices to enhance system reliability, sustainability, and resiliency.

FISCAL IMPACT:

The total fiscal impact associated with this Professional Consultant Services Agreement is $179,100, with an additional $150,000 of incidental services, as necessary, for a total of $329,100. The initial fiscal impact for Fiscal Year 2024-2025 is forecasted to be $60,000. Subsequent fiscal years are forecasted to be $60,000 in Fiscal Year 2025-2026 and $59,100 in Fiscal Year 2026-2027. Additionally, each year will include an additional amount of $50,000 for incidental services, as needed.

Projected cost share is 25% for each account. Sufficient funds are included in the Fiscal Year 2024/2025 – 2025/2026 budgets in the Legislative & Regulatory Risk Account No. 6025000-421000, Electric Operations Account No. 6100000-421000, Clearwater Generating Plant Account No. 6120140-421000, and Water Production & Operations Account No. 6200000-421000. Future fiscal years will be included as part of the subsequent budget process.

Prepared by:	Dr. Scott Lesch, Utilities Assistant General Manager/Power Resources
Approved by:	David A. Garcia, Utilities General Manager
Certified as to availability of funds:	Kristie Thomas, Finance Director/Assistant Chief Financial Officer
Approved by:	Rafael Guzman, Assistant City Manager
Approved as to form:	Jack Liu, Interim City Attorney

Attachments:

1. RFP Award Recommendation
2. Professional Consultant Services Agreement with AESI, Inc.
3. Presentation