PRODUCT DESCRIPTION (PD)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Infrastructure Operations (IO)

Schneider Electric EcoStruxure Power Monitoring Expert (PME)
Software, Maintenance, and Technical Support

Date: June 5, 2026
TAC Number: VA-27-00000904

DRAFT

PD Version Number: 1.0

CONTENTS

1.0 BACKGROUND 3
1.1 PRODUCT REQUIREMENTS 3
1.2 ORDER TYPE 3
1.3 PERIOD OF PERFORMANCE 3
1.4 PLACE OF PERFORMANCE 4
1.5 TRAVEL 8
2.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508) 8
2.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS 8
2.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY 8
2.3 ACCEPTANCE AND ACCEPTANCE TESTING 9
3.0 SHIPMENT OF SOFTWARE 9
4.0 GENERAL REQUIREMENTS 9
4.1 VA TECHNICAL REFERENCE MODEL 9
4.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS 9
4.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION 10
4.4 INTERNET PROTOCOL VERSION 6 (IPV6) 10
4.5 SOFTWARE AND LICENSING REQUIREMENTS 11
4.6 TRUSTED INTERNET CONNECTION (TIC) 11
4.7 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS 11

DRAFT

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information Technology (OIT), Infrastructure Operations (IO) requires software upgrade perpetual licensing—from 25 devices to 50 devices—along with continued maintenance and technical support for Schneider Electric (SE) EcoStruxure Power Monitoring Expert (PME) software. EcoStruxure PME collects system data from SE networked meters integrated throughout IO's data center support infrastructure, enabling critical monitoring of electrical performance and power quality. The requirement includes a perpetual software license (1–50 devices), ongoing maintenance and technical support, and access to Schneider Electric software engineering personnel familiar with IO's metered architecture and SE source code. This software is critical for collecting and analyzing power consumption, quality, and load flow data from proprietary SE networked meters currently deployed across VA data centers.

1.1 PRODUCT REQUIREMENTS

The Contractor shall provide one (1) telephone number and/or a point of contact for VA to contact and opening maintenance service calls. The vendor shall provide secure connection capabilities for the downloading of software updates and/or the uploading of diagnostic information. The preferred protocol for transfer is Secure File Transfer Protocol (SFTP).

Maintenance and support services shall include:

- Software updates (major, point, and service releases) on a quarterly basis, or within 48 hours for high-risk vulnerabilities patches.
- Bug fixes and upgrade assistance during normal business hours
- 12x5 email and online technical support, including access to new product downloads
- Secure connectivity for downloading updates and uploading diagnostic data

1.2 ORDER TYPE

This effort shall be proposed on a firm-fixed price basis.

1.3 PERIOD OF PERFORMANCE

The Period of Performance (PoP) is February 12, 2027 – February 11, 2028, to include two (2) 12-month option periods.

DRAFT

1.4 PLACE OF PERFORMANCE

Tasks under this PD shall be performed at the Austin Information Technology Center (AITC), located in Austin, Texas.

The Contractor shall provide the following:

Base Period: February 12, 2027 – February 11, 2028

Item No	Product Description	QTY	Unit
0001	Control No: SW5186.SVC Description: Digital Service Plan Prime Level License Metric: Lot License Duration: N/A OEM: Schneider Electric Mfg Part No: 197745601 Site No: [redacted] Customer No: (Act ID) 0007951654 HW Serial No: Not Available MCC: I00 AppCode: EDC Location: AITC	1	Each
0002	Control No: SW5186.SWM Description: Schneider Electric-EcoStruxure Power Monitoring Expert (PME) License (25 Devices) License Metric: Per Server License Duration: Perpetual OEM: Schneider Electric Mfg Part No: ESPPRIMENEW Customer No: 0007951654 HW Serial No: Not Available SW License Key: ACT-55AM-B79L-STLW-UPYF; PIN: 2692787 OEM Agreement No: PSC-1959298 MCC: I00 AppCode: EDC Location: [redacted]	1	Each
0003	Control No: SW5186.1SWMA Description: Schneider Electric-EcoStruxure Power Monitoring Expert (PME) License & ESP Edition: Standard	1	Each

DRAFT

Item No	Product Description	QTY	Unit
	License Metric: Per Server License Duration: Perpetual OEM: Schneider Electric Mfg Part No: ESPPRIMENEW Quantity: 1 (25-Device Pack, 2-Client Access) Site No: [redacted] Customer No: (Act ID) 0007951654 HW Serial No: Not Available SW License Key: ACT-55AM-B79L-STLW-UPYF; PIN: 2692787 Unique Vendor Ref ID: Virtual Machines (2) OEM Agreement No: PSC-1959298; PIN-2692787 MCC: I00 AppCode: EDC Location: [redacted]		
0004	Deliverable Support Information: The Contractor shall complete the Deliverable Support Information form (DSI) for maintenance support. The Contractor shall fill in blocks 15-32. Note for Multiple CLINs: For asset specific information that applies to multiple CLINs, provide an attachment correlating any asset specific information to specific CLINS. (For example: Serial Numbers or License Keys). The Contractor shall provide Original Equipment Manufacturer (OEM) confirmation that all software support or licenses have been purchased. The Contractor shall provide service call instructions to include all information required to obtain maintenance, support or licenses. The form shall be submitted electronically to: VA PM, COR, CO and AACLicense@va.gov	NSP	NSP

Option Period One: February 12, 2028 – February 11, 2029

Item No	Product Description	QTY	Unit
1001	Control No: SW5186.SVC Description: Digital Service Plan Prime Level License Metric: Lot License Duration: N/A OEM: Schneider Electric Mfg Part No: 197745601	1	Each

DRAFT

Schneider Electric EcoStruxure Power Monitoring Expert (PME)
Software, Maintenance, and Technical Support

Item No	Product Description	QTY	Unit
	Site No: AITC Customer No: (Act ID) 0007951654 HW Serial No: Not Available MCC: I00 AppCode: EDC Location: AITC		
1002	Control No: SW5186.SWM Description: Schneider Electric-EcoStruxure Power Monitoring Expert (PME) License (25 Devices) License Metric: Per Server License Duration: Perpetual OEM: Schneider Electric Mfg Part No: ESPPRIMENEW Customer No: 0007951654 HW Serial No: Not Available SW License Key: ACT-55AM-B79L-STLW-UPYF; PIN: 2692787 OEM Agreement No: PSC-1959298 MCC: I00 AppCode: EDC Location: [redacted]	2	Each
1004	Deliverable Support Information: The Contractor shall complete the Deliverable Support Information form (DSI) for maintenance support. The Contractor shall fill in blocks 15-32. Note for Multiple CLINs: For asset specific information that applies to multiple CLINs, provide an attachment correlating any asset specific information to specific CLINS. (For example: Serial Numbers or License Keys). The Contractor shall provide Original Equipment Manufacturer (OEM) confirmation that all software support or licenses have been purchased. The Contractor shall provide service call instructions to include all information required to obtain maintenance, support or licenses. The form shall be submitted electronically to: VA PM, COR, CO and AACLicense@va.gov	NSP	NSP

Option Period Two: February 12, 2029 – February 11, 2030

Item No	Product Description	QTY	Unit
2001	Control No: SW5186.SVC Description: Digital Service Plan Prime Level	1	Each

DRAFT

Schneider Electric EcoStruxure Power Monitoring Expert (PME)
Software, Maintenance, and Technical Support

Item No	Product Description	QTY	Unit
	License Metric: Lot License Duration: N/A OEM: Schneider Electric Mfg Part No: 197745601 Site No: [redacted] Customer No: (Act ID) 0007951654 HW Serial No: Not Available MCC: I00 AppCode: EDC Location: AITC		
2002	Control No: SW5186.SWM Description: Schneider Electric-EcoStruxure Power Monitoring Expert (PME) License (25 Devices) License Metric: Per Server License Duration: Perpetual OEM: Schneider Electric Mfg Part No: ESPPRIMENEW Customer No: 0007951654 HW Serial No: Not Available SW License Key: ACT-55AM-B79L-STLW-UPYF; PIN: 2692787 OEM Agreement No: PSC-1959298 MCC: I00 AppCode: EDC Location: [redacted]	2	Each
2004	Deliverable Support Information: The Contractor shall complete the Deliverable Support Information form (DSI) for maintenance support. The Contractor shall fill in blocks 15-32. Note for Multiple CLINs: For asset specific information that applies to multiple CLINs, provide an attachment correlating any asset specific information to specific CLINS. (For example: Serial Numbers or License Keys). The Contractor shall provide Original Equipment Manufacturer (OEM) confirmation that all software support or licenses have been purchased. The Contractor shall provide service call instructions to include all information required to obtain maintenance, support or licenses. The form shall be submitted electronically to: VA PM, COR, CO and AACLicense@va.gov	NSP	NSP

DRAFT

1.5 TRAVEL

The Government does not anticipate travel under this effort to perform the tasks associated with the effort throughout the PoP.

2.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

2.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request, or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☐ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

2.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be

DRAFT

compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

2.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

3.0 SHIPMENT OF SOFTWARE

Ship To and Mark For: Delivery of software licenses and/or maintenance shall be submitted electronically. Delivery of DSI form shall be sent to [redacted] (see Deliverable Support Information CLIN) and provide notice to:

Name: [redacted]
Address:
Email:
[redacted]

4.0 GENERAL REQUIREMENTS

4.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

4.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls

DRAFT

cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

4.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the Integrated Control Number (ICN) in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

4.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 "USGv6 Profile" (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6" (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

DRAFT

4.5 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor's proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

4.6 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative" (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 "Secure External Connections", and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents.)

4.7 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

If Artificial Intelligence (AI) is part of the Contractor system/solution, the Contractor shall be in compliance with E.O. 13960 and 14319, OMB Memorandums M-25-21, M-25-22, and M-26-04, and VA Directive and Handbook 6500 to support VA in trustworthy, secure, responsible, accountable, Truth Seeking, and Ideologically Neutral AI innovation.

No web-based, publicly available generative AI service has been approved for use with VA-sensitive data including, but not limited to OpenAI's ChatGPT, Microsoft's Copilot, Google's Gemini, and Anthropic's Claude. No PII, protected health information (PHI), or VA-sensitive data should be entered into these unapproved services. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23). The Contractor shall protect VA Sensitive data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from VA.

The Contractor shall deliver the services, technical data, configurations, models, weights, documentation or other information, including source code, developed during contract performance. The Contractor, in collaboration with VA, must evaluate the output of any AI tool for accuracy prior to using the output in VA efforts. All data, including models, weights, algorithms, and outputs generated using either Government-furnished data or data first developed under this contract shall be the property of the Government with unlimited rights as defined by FAR 52.227-14. The Contractor shall also deliver any custom-developed code developed with AI methodologies in accordance with the SHARE IT Act, if applicable. VA shall also retain unlimited rights to

any improvements to that data, including the continued design, development, testing, and operation of AI systems and/or systems utilizing AI.

The Contractor shall ensure that all AI Systems, including Large Language Models (LLM), whether standalone LLMs or integrated into broader software platforms, procured under this effort and/or used in performance of this contract complies with the Unbiased AI Principles as defined in Executive Order 14319 and OMB Memorandum M-26-04, e.g. Truth Seeking and Ideologically Neutral, as applicable to the intended use of the system.

The Contractor shall ensure that AI System/LLM generated outputs are truthful in responding to user prompts seeking factual information or analysis, prioritize historical accuracy, scientific inquiry, and objectivity, as well as acknowledge uncertainty where reliable information is incomplete or contradictory and do not fabricate, hallucinate, or present unverifiable information as fact.

The Contractor shall ensure that LLMs and AI outputs are neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as Diversity, Equity, and Inclusion (DEI). The Contractor shall ensure that the LLMs, including the AI System, are not intentionally encoded with partisan or ideological judgments within an AI System's/LLM's outputs unless those judgments are prompted by or otherwise readily accessible to the end user.

Compliance with the AI requirements of this contract, including adherence to the Unbiased AI Principles, Truth-Seeking and Ideological Neutrality requirements, disclosure obligations, monitoring and reporting requirements, and corrective action responsibilities, is a material condition of eligibility for payment and continued performance. In accordance with OMB Memorandum M-26-04, failure to comply with these requirements, or refusal to take timely and appropriate corrective action to remedy identified noncompliance, may constitute a material breach of contract and may result in remedies consistent with the terms of the contract and applicable law including but not limited to withholding of payment, termination for cause/default, or other appropriate contractual remedies, as determined by the Contracting Officer.

All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation as identified in the Artificial Intelligence in VA Contracts clause, to include its associated list of AI being used in contract performance.

Deliverable:

A. Statement of Attestation

DRAFT

POINTS OF CONTACT

[redacted]

DRAFT

INFORMATION SECURITY CONSIDERATIONS

The Assessment and Authorization (A&A) requirements do not apply and a Security Accreditation Package is not required.

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this Product Description.

DRAFT