



Date: December 19, 2025

To: All Vendors

Subject: Addendum #4

REFERENCE: P008-26 BPUB INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY COLLABORATION STRATEGY

This Addendum forms part of the contract and clarifies, corrects or modifies original RFP document.

NEW SUBMISSION DATE & TIME: January 30, 2026 by 3:00 PM

NEW OPENING DATE & TIME: January 30, 2026 at 3:15 PM

NOTE: REMOVE LINE ITEM (a) UNDER MINIMUM QUALIFICATIONS:

- (a) Be independent and non-product affiliated. This does not prohibit the firm from recommending a product or products.

Question 1: Please define the expected data sources, data types, update frequency, approximate volumes, and any regulatory data classifications associated with the IT/OT data-sharing use cases. (Reference: RFP Page 14–15, collaborative data requirements.)

Answer 1:

Data sources: Operational Data, Internal Systems.

Data types: Structured, semi-structured.

Update frequency: Real-time.

Approximate volumes: up to 100mbps data transfer. A couple of terabytes of storage per year.

Regulatory data classifications: Still to determine but could include NERC defined Bulk Electric System Cyber System Information (BCSI) confidential data and internal data.

Question 2: Please clarify what CIP-protected assets, networks, or data the consultant may access, and what restrictions, training, or authorization requirements apply. (Reference: Electric SCADA governed by NERC CIP.)

Answer 2: The consultant will not access any CIP-protected assets or networks. However, it is likely that the consultant will need access to BCSI (BES Cyber System Information). BPUB internal procedure requires that before granting access to BCSI, the consultant(s) will need to complete BPUB provided training on identification, protection and usage of information classified as BCSI. This training can take up to 8 hours to complete. In addition, BPUB requests attestation of personnel background checks not older than seven years for all personnel that will access BCSI.

Question 3: Does BPUB already have a preferred architectural pattern for IT/OT collaboration (e.g., unified data platform, historian integration, DMZ broker, middleware, cloud broker)? (Reference: RFP 2.2 requires meeting IT and OT to discuss their “preferred collaboration methodology.”)

Answer 3: BPUB as a whole does not already have a preferred architectural pattern for IT/OT collaboration but each department has a preference on the architectural plan. The consultant is required to discuss such plans with each department and suggest an architecture plan that satisfies both departments.

The SCADA department would like to place strong emphasis in the Purdue model and Zero Trust model with micro segmentation.

IT's preferred collaboration data platform is Zscaler which is a cloud-based cybersecurity company providing a Zero Trust Exchange platform that secures internet access, cloud apps, and private applications for businesses.

Question 4: Please specify the exact cybersecurity and regulatory frameworks the consultant must align with (NERC CIP versions, DHS directives, CISA guidance, cyber-insurance requirements, or Texas-specific utility cybersecurity standards). (Reference: RFP requires compliance with “NERC, DHS, Cybersecurity insurance companies, etc.”)

Answer 4:

NIST CSF 2.0

NERC CIP-002-5.1a

NERC CIP-003-8

NERC CIP-004-7

NERC CIP-005-7

NERC CIP-006-6

NERC CIP-007-6

NERC CIP-008-6

NERC CIP-009-6

NERC CIP-010-4

NERC CIP-011-3

NERC CIP-012-1

NERC CIP-013-2

NERC CIP-014-3

NERC CIP-015-1

IT's framework is based on the NIST framework which also includes internal policies, procedures and work instructions. IT department currently participates in a DHS program, providing weekly Cyber Hygiene reports and Cyber Resilience Review (CRR) Self-Assessments. Annual Penetration Test required by BPUB's cybersecurity procedure meeting insurance requirements.

Question 5: Should the consultant provide implementation-level engineering detail—including configurations, bills of material, and network/component specifications—or should deliverables remain strictly strategic in nature? (Reference: RFP states consultant “will not perform actual implementation” yet requests detailed configuration and policy recommendations.)

Answer 5: The deliveries should remain strictly strategic.

Question 6: What specific system access (network diagrams, architecture documents, cloud environments, test systems, asset lists) will BPUB provide during discovery? (Reference: RFP notes dependence on receiving “existing, available, and necessary data.”)

Answer 6: SCADA will provide network diagrams, architecture documents, assets list and other documentation as needed. IT will provide network diagrams, architecture documents, assets list and other documentation as needed.

Question 7: Will any Personal Information or Highly Sensitive Personal Information—per Exhibit D definitions—be included in the IT/OT collaboration data flows? If so, what data types and required protections should be assumed? (Reference: Exhibit D definition of PI and Highly Sensitive PI.)

Answer 7: SCADA does not expect or plan to include Protected Personal Information and Highly Sensitive Personal Information in the collaboration data flows. IT does not expect to include any PPI in this collaboration.

Question 8: What level of accuracy and granularity does BPUB expect for the capital, O&M, and staffing estimates (ROM %, preliminary engineering-level, or detailed)? (Reference: Deliverable requiring “Estimated capital, O&M, and human resource expenses.”)

Answer 8: BPUB expects a Level 4 (Study/Conceptual) estimate.

Question 9: Please identify which departments, roles, or stakeholder groups the consultant is expected to interview, as well as anticipated participation levels or time commitments. (Reference: RFP requires meeting “BPUB departments,” IT, OT, and user groups.)

Answer 9: For the SCADA department, the consultant is expected to interview and get participation from the SCADA manager, SCADA Cybersecurity architect, SCADA network administrators and SCADA systems analysts. Several hours a week can be allocated for the project.

The consultant selected is expected to interview personnel from the IT software, hardware and cybersecurity teams as needed.

Question 10: Please provide a list of planned future projects, systems, or initiatives that will require IT/OT data interoperability so the strategy can appropriately account for them. (Reference: RFP notes “future projects will require interconnectivity” but does not specify which ones.)

Answer 10:

SEL Blueframe Implementation

OMS/EMS Integration

DMS/EMS Integration

AMI/EMS Integration

Water SCADA Dashboards

Security & Safety Video

Security Access Controls

End-users have a need to access information from applications and collection of data from the IT/OT networks.

Question 11: To ensure accurate pricing and reduce proposal variance, can BPUB provide the anticipated budget range or internal not-to-exceed amount allocated for the IT/OT Collaboration Strategy project?

Answer 11: There is not a proposed not-to-exceed amount allocated. BPUB is interested in seeing projected estimates that will be used to justify funding from executive management.

Question 12: Could BPUB elaborate on the key business drivers motivating the development of an IT/OT Collaboration Strategy?

Answer 12: The increased complexity and interconnectivity requirements of systems and departments requires a corporate level strategy to guide the process from planning all the way to implementation of current and future projects.

Question 13: Are there upcoming initiatives, regulatory requirements, or software deployments that specifically require deeper IT/OT interoperability?

Answer 13: Yes, there are upcoming initiatives and software deployments that require deeper IT/OT interoperability. See response to question 10.

Question 14: What SCADA platforms are currently used across Electric, Water, and Wastewater systems?

Answer 14: For Electric SCADA, Emerson's OSI EMS is currently in use, with SEL field equipment (RTACs, Relays).

For Water & Wastewater, Rockwell Software Factory Talk View SE Platform & Allen Bradley Controllers.

Question 15: What security technologies (firewalls, SIEM, IDS/IPS, endpoint protection, identity management, etc.) are deployed today in IT and OT?

Answer 15:

SCADA has the following for the OT side:

Firewalls: Cisco ASA and Fortigate.

SIEM: SolarWinds Security Manager

IDS/IPS: Cisco FirePOWER, Fortigate IPS.

Endpoint protection: Symantec Endpoint Protection

Identity Management: Microsoft AD.

Vulnerability Management: Qualys

IT department has consolidated to Palo Alto Networks as their security platform. Platform includes centralized cloud data logs, managed threat hunting, Cortex XDR, and Unit 42 as the incident response provider.

Question 16: Does BPUB utilize a central data warehouse, data lake, historian, or similar data platform?

Answer 16: Electric SCADA utilizes the OSI historian DataHis, for the EMS system.

WWW SCADA utilizes the Rockwell Factory Talk Historian.

Addendum #4 - P008-26 BPUB IT and OT Collaboration Strategy

Question 17: Is BPUB currently using any cloud infrastructure (AWS, Azure, or private cloud)?

Answer 17: SCADA is not using cloud infrastructure.

IT has implemented a hybrid on-prem and Azure cloud infrastructure. IT currently also has some applications in a SaaS environment. The plan is to continue migrating applications to the cloud environment.

Question 18: Is there an existing data governance or data classification framework in place?

Answer 18: Electric SCADA follows NERC CIP-011 data classification requirements.

WWW SCADA does not have a data governance or data classification framework in place.

The IT network has strict data governance and data classification based on systems, roles and profiles. IT follows a least privileged methodology.

Question 19: What is BPUB's current NERC CIP applicability (e.g., low impact, medium impact assets)?

Answer 19: BPUB has low and medium impact rated facilities and associated assets.

Question 20: Has BPUB undergone recent NERC CIP audits or assessments that should inform our approach?

Answer 20: The Electric SCADA system is audited every three years. We are in a current audit for FY2026.

The Electric SCADA system had an assessment done in 2024 by the NATF and Palo Alto's Unit 42 division. Recommendations for improvement have been implemented. Access to the assessments can be shared with the awarded vendor once appropriate NDA has been signed.

Question 21: Which DHS/CISA or other federal cybersecurity standards or directives apply to BPUB's OT systems?

Answer 21: No DHS/CISA federal cybersecurity standards apply to BPUB's OT systems. However, other NERC standards may apply, like EOP or TOP. IT is enrolled and collaborates with DHS programs and standards.

Question 22: Is BPUB pursuing or considering a Zero Trust security model?

Answer 22: Yes.

Question 23: Are there existing governance processes for change management, configuration management, and incident response across both domains (IT/OT)?

Answer 23: No.

Question 24: Which departments and user groups are requesting greater access to operational data?

Answer 24: Electric Engineering, Electrical Substations and Relaying, WWW Engineering, WWW Operations, Customer Service, Executive Management.

Addendum #4 - P008-26 BPUB IT and OT Collaboration Strategy

Question 25: What specific operational datasets (electric, water, wastewater, financial, customer, etc.) are needed for collaboration?

Answer 25: Electric, water, wastewater, customer, financial, GIS, AMI, fleet.

Question 26: What level of data synchronization is expected—real-time, near real-time, or periodic?

Answer 26: Real-time/near real-time is expected.

Question 27: What data-sharing mechanisms are preferred or currently under evaluation (APIs, historians, data fabric, ETL pipelines, etc.)?

Answer 27: Historians and APIs.

Question 28: Does BPUB expect bidirectional data sharing between IT and OT, or read-only access from IT into OT systems?

Answer 28: Most projects will require read-only access from IT into OT systems.

Question 29: Does BPUB use a historian platform such as OSIsoft PI or similar?

Answer 29: Electric SCADA currently uses OSI's monarch historian with a planned upgrade to the Chronus historian.

WWW SCADA currently uses Rockwell Factory Talk Historian.

Question 30: Does BPUB require a proof-of-concept design or only high-level planning recommendations?

Answer 30: High-level planning.

Question 31: Is BPUB expecting vulnerability scanning or primarily architectural/security review?

Answer 31: BPUB is expecting an architectural/security review.

Question 32: Which cybersecurity frameworks does BPUB prefer for alignment (NIST CSF, NIST 800-53, CIS Controls, NERC CIP, ISO 27001, ISA 62443)?

Answer 32: Electric SCADA prefers alignment with NERC CIP.
WWW SCADA prefers alignment with NIST CSF NIST 800-82r3.
IT prefers alignment with NIST CSF.

Question 33: Is BPUB expecting full policy revisions or gap-based recommendations?

Answer 33: SCADA is expecting gap-based recommendations however, IT is not expecting any policy revisions.

Question 34: Are onsite activities required, or can the project be executed remotely/hybrid?

Addendum #4 - P008-26 BPUB IT and OT Collaboration Strategy

Answer 34: The project can be executed remotely.

Question 35: Are there operational blackout periods or restricted times for interviews, walkthroughs, or assessments?

Answer 35: No.

Question 36: Does BPUB have a preferred timeline for completion beyond what is stated in the RFP?

Answer 36: BPUB would like to complete the project as soon possible with the understanding that the delivery date might be prolonged based on data requests delivery. Beyond that, BPUB does expect for the project to be completed within a reasonable time after data delivery.

Question 37: Will the Board of Directors require a public presentation beyond the standard deliverables?

Answer 37: No.

Question 38: Does BPUB have a target budget range or ceiling for this engagement?

Answer 38: No.

Question 39: Are subcontractors permitted, and must they be declared at submission time?

Answer 39: Subcontractors are permitted at your discretion, but must be vetted by you under your responsibility.

Question 40: What are BPUB's top operational pain points today (e.g., asset downtime, reporting latency, compliance overhead, outage response)?

Answer 40: Reporting latency, outage response, lack of operational visibility or situational awareness during emergency events.

Question 41: Is BPUB envisioning IT/OT integration primarily for internal analytics and reporting, or also to support external stakeholders (state regulators, emergency services, public dashboards)?

Answer 41: To support external stakeholders as well.

Question 42: What is the cost or efficiency goals driving this project (e.g., target reduction in manual data handling or compliance effort)?

Answer 42:

Reduce outage troubleshooting times.

Reduce outage downtime.

Reduce customer outage reporting calls.

Increase customer satisfaction ratings.

Reduce driving hours.

Addendum #4 - P008-26 BPUB IT and OT Collaboration Strategy

Reduce compliance risk
Increase situational awareness, decision making process.

Question 43: Are there performance metrics (KPIs) BPUB expects to track after implementation?

Answer 43: Not for the specific IT/OT implementation. (Suggested metrics are welcomed).

Question 44: How segregated are IT and OT networks today?

Answer 44: 100% segregated.

Question 45: Are there existing interconnects or DMZ zones between the two domains?

Answer 45: There are currently no existing interconnects.

Question 46: What protocols and communication standards are used in OT?

Answer 46: Electric SCADA Protocols: DNP, SEL protocol. Communication standards: RS-232, TCP/IP.

WWW SCADA Protocols: Allen Bradley Ethernet I/P. Communication standards TCP/IP.

Question 47: Does BPUB employ asset discovery or network monitoring tools?

Answer 47: SCADA utilizes Solarwinds NPM, PRTG. IT has an asset management solution and does utilize network monitoring tools.

Question 48: Is remote vendor access to OT environments allowed today? If yes, how is it controlled or logged?

Answer 48: Vendor access is not allowed in either Electric SCADA or WWW SCADA OT environments.

Question 49: Are any data ingestion mechanisms already in use?

Answer 49: Neither Electric SCADA nor WWW SCADA have any data ingestion mechanisms other than the current SCADA/EMS system.

Question 50: Does BPUB use a message bus or middleware layer for event/data exchange?

Answer 50: BPUB uses ICCP for data exchange with external stakeholders. In regards to internal data, the SCADA systems acquire data directly from field devices through their respective data servers. No middleware is utilized for data exchange.

Question 51: Are there any data sovereignty or residency requirements restricting where data can be stored or processed?

Answer 51: Yes. For Electric SCADA, CIP-011 mandated the identification of designated storage locations of BCSI, be it on-prem, cloud or hybrid.

Addendum #4 - P008-26 BPUB IT and OT Collaboration Strategy

For the WWW SCADA system there is no regulatory compliance, but BPUB prefers to keep the data onsite at our storage servers in our data centers.

Question 52: Is there a canonical data model or semantic layer for operations data?

Answer 52: Electric SCADA does not have a canonical data model or semantic layer for operations data.

Question 53: Does BPUB maintain a data catalog or metadata repository?

Answer 53: Neither Electric SCADA nor WWW SCADA have a data catalog or metadata repository.

Question 54: The RFP includes a Sample Agreement. Can you confirm whether vendors are expected to adhere to the terms and conditions of this Sample Agreement upon proposal submission?

Answer 54: Yes. If agreement is redlined, BPUB's Legal Department will review the redlined document.

Question 55: If adherence is required, will vendors be permitted to propose modifications or exceptions as part of their submission?

Answer 55: Yes.

Question 56: Will there be an opportunity to negotiate the agreement terms post-award?

Answer 56: Agreement should be redlined and included in your submission for BPUB Legal review.

Question 57: Could BPUB clarify the anticipated duration of the IT/OT Collaboration Strategy project? The RFP outlines the required tasks and deliverables, but it does not specify an estimated project end date or expected timeframe for completion.

Answer 57: Anticipated duration of the project is not included due to unfamiliarity with the time required to complete such an assessment. Please provide an expected timeframe for completion.

Question 58: What SCADA solutions are currently in use for Electric and Water?

Answer 58: For Electric SCADA: OSI Monarch EMS.
For WWW SCADA: Rockwell Software Factory Talk View SE

Question 59: This request includes network architecture only. Is data pipelining (data analysis, acquisition, historian, etc.) out of scope for this effort?

Answer 59: Yes, data pipelining is out of scope.

Question 60: Can BPUB identify which cloud services, if any, are currently in use and whether there is a preferred cloud provider?

Answer 60: Neither Electric SCADA nor WWW SCADA have any cloud services. IT already has Microsoft Azure for cloud services. Other departments use other SaaS environments.

Question 61: What is the approximate number of IT and OT stakeholders expected to participate in the assessment?

Answer 61:

OT Stakeholders: 9

IT Stakeholders: 8

Question 62: Is NERC CIP compliance experience a mandatory requirement for proposing, or is it considered a preferred qualification?

Answer 62: NERC experience is preferred, otherwise at a minimum, a certification from a NERC CIP Standard bootcamp or similar training would be required. The idea here is that at a minimum, the consultant must have certified knowledge of the NERC CIP Standards in regards to data handling.

Question 63: Could you share whether BPUB has established a budget range or an anticipated spending target for this effort?

Answer 63: No budget range has been established.

The signature of the company agent, for the acknowledgement of this addendum, shall be required. **Complete information below and return via e-mail to: MaGaytan@brownsville-pub.com.**

I hereby acknowledge receipt of this addendum.

Company: _____

Agent Name: _____

Agent Signature: _____

Address: _____

City: _____ **State:** _____ **Zip:** _____

Phone Number: _____ **E-mail address:** _____

If you have any further questions about the RFP, call 956-983-6365.

BY: *Diane Solitaire*
Purchasing Department