Table of Contents

American Public Power Association

Request for Proposal (RFP):

Design, Implementation, and Managed Operations of a Secure Azure Government (GCC High) Environment

Invitation to Submit Proposal

The American Public Power Association (APPA) invites qualified and experienced Contractors to submit proposals for the design, implementation, and management of a secure Microsoft Azure Government (GCC High) environment.

This RFP is based upon work supported by the Department of Energy under Award Number DE-CR0000026.

Introduction and Background

The Department of Energy entered into a cooperative agreement with APPA under Award Number DE-CR0000026 to support efforts to improve the cybersecurity posture of public power utilities. This effort is focused on strengthening cybersecurity capabilities across the public power sector and enabling utilities to better manage and respond to evolving cyber threats. As part of this effort, APPA requires a secure environment built on zero trust principles to support controlled access to the Cybersecurity Accelerator Program (CAP).

CAP is intended to support cybersecurity maturity, information protection, and secure data handling for participating public power utilities. To enable this work, APPA requires a secure and isolated information technology environment that is designed, implemented, and operated in accordance with elevated cybersecurity requirements.

American Public Power Association Background

APPA serves over 2,000 community- and state-owned electric utilities. APPA provides representation, information, counseling, and other services in the areas of:

- Federal legislation, rules, and regulations
- Engineering and operations, including risk management activities
- Accounting and finance
- Marketing trends
- New technologies
- Human resources
- Customer services
- Energy research
- Communications
- Energy services

Founded in 1940, APPA works in partnership with the nation's public power utilities to help increase productivity, control rates, protect their community's investment in public power, and enhance their ability to compete.

Through this RFP, APPA seeks a Contractor to design, implement, and operate a secure, dedicated environment hosted in the Microsoft Azure Government cloud. The environment must meet applicable cybersecurity, compliance, and operational requirements and align with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 for the protection of high-risk data.

The environment will support access for up to two dedicated laptops configured exclusively for this project. These endpoints will be tightly controlled and restricted to approved use cases. APPA will retain overall governance, risk management, and compliance oversight, while the selected Contractor will be responsible for technical execution, secure implementation, and ongoing operational support as defined in this RFP.

Refer to Appendix A for a high-level architectural design of the desired environment.

Security Considerations

Given the importance of protecting sensitive information and operating a secure zero trust environment, APPA is seeking a Contractor and solution that applies zero trust security principles across identity, devices, networks, workloads, and data. The proposed solution must enforce continuous verification, least privilege access, strong identity and device validation, network segmentation, and comprehensive monitoring.

The Contractor must implement security controls aligned with an industry-accepted security framework or control set, such as NIST SP 800-171 or the NIST Cybersecurity Framework (CSF) 2.0, and demonstrate effective implementation of those controls through independent validation or third-party assessments. The zero trust environment must be designed to prevent

implicit trust, restrict lateral movement, and ensure that access to systems and data is continuously evaluated and auditable.

Project Objectives

- By July 31, 2026, design and implement a secure and isolated Microsoft Azure Government (GCC High) environment aligned with APPA's approved high risk cybersecurity requirements and a zero trust security model.
- Ensure the environment and associated endpoints comply with NIST SP 800-171 and applicable cybersecurity best practices.
- Provide secure and auditable access to the environment through up to two dedicated laptops configured with least functionality and strong access controls.
- Operate and maintain the environment through defined security operations, monitoring, patching, configuration management, and support processes.
- Enable APPA to demonstrate continuous compliance, effective control execution, and audit readiness throughout the project lifecycle.

Terms and Deadlines

The term of the contract will start on the date of execution and shall continue until April 30, 2028. While there will be a key deadline of July 31, 2026, for design, configuration and implementation, APPA is seeking continued support for maintaining and operating the environment. The schedule for any additional deliverables beyond initial implementation will be agreed upon in writing by APPA and the selected Contractor. APPA may seek to renew this contract beyond the specified end date at a later time.

Ownership

All components of the environment including but not limited to data, licenses, tenants, documentation, developed or received by the Contractor pursuant to the contract shall become the exclusive property of APPA and shall be delivered to APPA upon request of the APPA program manager or upon termination of the Contract, whichever is earlier. The Contractor can only use these components for the purpose of fulfilling its obligations under the contract and is expressly prohibited from selling, licensing, or otherwise transferring any data obtained as part of the contract to any third party unless by written request from APPA. The Contractor is also prohibited from using, disclosing, or retaining any data for its own business purposes.

Roles and Responsibilities

I. Role of the Contractor

The Contractor shall be responsible for the design, implementation, operation, and ongoing support of the secure Azure Government (GCC High) environment in accordance with the

requirements of this RFP. Contractor responsibilities include, but are not limited to, the following:

- Designing, implementing, securing, and operating a secure and isolated Azure Government (GCC High) environment aligned with APPA approved high risk cybersecurity requirements, NIST SP 800-171, and zero trust security principles.
- Completing all required implementation activities within the timeframes specified in this RFP.
- Configuring, hardening, and managing all cloud resources, security controls, and supporting infrastructure necessary to maintain a secure, segmented environment.
- Configuring, securing, and managing up to two dedicated and locked down laptops, including endpoint security, centralized device management, secure connectivity, and enforcement of least functionality.
- Providing ongoing operational support in accordance with defined support hours and service level requirements, including security monitoring, patch and vulnerability management, configuration and change control, incident response support, and maintenance of required technical and compliance documentation.
- Participating in scheduled project status meetings to review progress, risks, operational status, and planned changes with APPA staff.
- Developing and maintaining technical documentation, operational runbooks, and security artifacts necessary to support audit readiness, operational continuity, and knowledge transfer to APPA.

II. Role of APPA

APPA will serve in an oversight, governance, and coordination role throughout the engagement. APPA responsibilities include, but are not limited to, the following:

- Providing overall project governance, cybersecurity oversight, and approval of key design decisions, deliverables, and material changes to scope or architecture.
- Working with the Contractor following contract award to establish project timelines, milestones, and communication protocols.
- Reviewing and approving deliverables, documentation, and reports submitted by the Contractor in accordance with the agreed-upon project plan.
- Managing contractual matters, internal coordination, and stakeholder communication related to the engagement.
- Managing costs associated with approved platform usage, licensing, and services as defined in the contract.

Zero Trust Environment Requirements

Period of Performance

The period of performance for this engagement shall commence on the date of contract award and continue through April 30, 2028. All tasks, deliverables, and activities under this engagement are subject to review and adjustment by APPA, in coordination with the Contractor, to ensure continued alignment with program needs and cybersecurity requirements.

General Scope Requirements

The Contractor shall be responsible for the full lifecycle design, implementation, operation, maintenance, and procurement or coordination of procurement of all required platform licenses, subscriptions, and services necessary to deliver and support a secure Microsoft Azure Government (GCC High) environment in accordance with APPA's approved cybersecurity requirements.

Technical and Operational Requirements

The scope of work includes the following:

Cloud Platform and Core Services

The Contractor shall design, implement, continuously enforce, and operate the Zero Trust Environment (ZTE) consistent with APPA approved high risk cybersecurity plan using Microsoft Azure Government (GCC High). This includes Azure Virtual Networks, Azure Firewall or Azure Government approved network security controls, Azure Storage (Government), and Azure Backup (Government). At a minimum, the Contractor shall implement the following non-negotiable controls below:

Identity and Access Management

The Contractor shall implement and manage identity and access controls using Microsoft Entra ID (Azure Active Directory Government). This includes conditional access policies, multi-factor authentication (MFA), and role based access control, implemented in accordance with least privilege principles. Identity and Access Enforcement shall include but not be limited to:

- Access shall be granted only after continuous verification of user identity, device posture, and session context.
- MFA shall be required for all access.
- Least privilege and separation of duties shall be enforced at all times.

Endpoint Configuration and Management

The Contractor shall configure, harden, and manage up to two dedicated laptops using Microsoft Intune (Government) and Windows Autopilot (Government). Endpoint requirements include full disk encryption using BitLocker, application allow listing, centralized device management, and enforcement of least functionality. Endpoint Restrictions shall include but not limited to:

- Endpoints shall be locked down to allow execution only of explicitly approved applications (deny-by-default).
- No web browsing, email clients, or cloud-based productivity applications shall be permitted on ZTE endpoints.
- No user-installed software shall be permitted.

Protocol and Network Controls

- NTLM authentication, SMB file sharing, and other legacy or insecure protocols shall be explicitly disabled.
- All data shall be encrypted in transit and at rest using NIST-approved cryptographic standards.
- Endpoints shall connect only to explicitly authorized ZTE resources and approved backend platforms.
- Micro-segmentation shall be enforced to prevent lateral movement.

Security Monitoring and Logging

The Contractor shall implement centralized security monitoring and logging using Microsoft Sentinel (Government), Azure Monitor, and Log Analytics (Government) to support threat detection, auditability, and incident investigation. Monitoring and Logging shall include but not be limited to:

- All authentication attempts, access events, configuration changes, and data transfers shall be logged and monitored centrally.
- Logs shall be protected from modification and retained in accordance with NIST SP 800-171 requirements.

The Contractor shall document this baseline and demonstrate enforcement as part of implementation of acceptance and ongoing operations.

3rd Party Platform Integration

The Contractor shall be responsible for securely integrating the Zero Trust Environment with the CAP backend platform.

The Contractor's responsibilities shall include, but are not limited to:

- Secure design and enforcement of all data exchange mechanisms.

- Implementation of strict data flow controls to ensure that only authorized data is transmitted.
- Centralized logging and monitoring of all integration activity.
- Enforcement of encryption and authentication controls for all data in transit.
- Participation in coordinated incident response activities involving the backend platform provider.

The Contractor shall be accountable for the security of all data in transit between APPA-managed endpoints, the Zero Trust Environment, and the backend platform, regardless of backend platform ownership.

Threat Protection and Endpoint Security

The Contractor shall deploy and operate Microsoft Defender for Endpoint (Government) and Microsoft Defender for Cloud (Government) to provide endpoint protection, threat detection, and continuous monitoring of the security posture.

Patch and Configuration Management

The Contractor shall perform ongoing patch management, vulnerability remediation, and configuration management using Microsoft Intune (Government).

Secure Connectivity

The Contractor shall provide secure, always on connectivity using Azure VPN Gateway (Government) or equivalent Azure Government approved VPN services. Connectivity shall include but not be limited to:

- Always-on VPN connectivity shall be enforced.
- Internet egress shall be restricted explicitly to the CAP online platform and other approved destinations only.

Operational Support and Documentation

The Contractor shall provide ongoing operational support, including incident response assistance, configuration and change control, and maintenance of required documentation. Documentation includes configuration baselines, audit logs, security control evidence, and operational runbooks.

Contractors proposing alternative tools must demonstrate that such tools are fully compatible with Azure Government (GCC High) and must provide written justification for any proposed deviations.

Continuity of Operations and Recovery Testing

The Contractor shall document and maintain continuity of operations and recovery procedures applicable to the Zero Trust Environment.

At a minimum, the Contractor shall:

- Document recovery procedures for ZTE components.
- Conduct at least one recovery or continuity test annually.
- Provide APPA with a summary of test results and corrective actions.

Continuity and recovery planning shall be appropriate to the sensitivity and availability requirements of the environment.

Compliance and Security Requirements

All solutions must be hosted exclusively within Microsoft Azure Government (GCC High). Use of commercial Azure environments is not permitted.

The environment must meet the security requirements of NIST 800-171 for non-federal systems handling high risk data.

All security controls and operational practices must align with APPA's approved cybersecurity requirements.

Storage, processing, or access to project data outside approved environments is strictly prohibited.

Vulnerability Management and Penetration Testing Requirements

The Contractor shall implement a continuous vulnerability management program for all ZTE components.

At a minimum, the Contractor shall:

- Perform automated vulnerability scanning on a recurring basis.
- Provide APPA with written vulnerability scan reports on a monthly basis.
- Remediate identified vulnerabilities based on severity and risk.

In addition, the Contractor shall ensure that an independent penetration test of the Zero Trust Environment is conducted at least annually. Penetration testing scoping, results and remediation evidence shall be provided to APPA.

Contractor Requirements

Contractors responding to this RFP must meet the following requirements:

- Proven experience designing, implementing, and operating secure environments in Microsoft Azure Government (GCC High).
- Demonstrated expertise implementing and maintaining security controls aligned with NIST Special Publication 800-171 using Microsoft security and management tooling.
- Hands on experience with Microsoft Azure Government core services, Microsoft Entra ID, Microsoft Intune and Windows Autopilot, Microsoft Sentinel, Azure Monitor, Log Analytics, Microsoft Defender for Endpoint, Microsoft Defender for Cloud, and Azure VPN Gateway.
- Experience securing and managing locked down endpoints in regulated or high-risk environments.
- Ability to provide ongoing operational, security, and compliance support using United States based personnel only.
- Demonstrated capability to produce and maintain audit ready documentation, including security control evidence and operational runbooks.
- Ability to provide a current SOC 2 Type 2 report on an annual basis for the duration of the contract.
- All Contractor personnel who design, implement, administer, monitor, maintain, or support the environment described in this RFP must be physically located within the United States. This requirement applies to all roles, including but not limited to cloud engineers, system administrators, security analysts, help desk staff, and management personnel with access to project systems or data.
- No offshore, near-shore, or non-U.S.-based personnel may access the Azure Government (GCC High) tenant, subscriptions, virtual networks, security tooling, logs, endpoints, credentials, or project data.
- Remote access to the environment must originate from within the United States, and access must be restricted through role-based access controls and least privilege principles.
- The Contractor must maintain controls to prevent unauthorized geographic access and must promptly notify APPA of any staffing or access changes that could impact compliance with this requirement.
- APPA reserves the right to require written attestations, staffing documentation, and audit evidence to validate compliance. Failure to comply with this requirement may result in disqualification of the proposal or termination of the resulting contract.
- Must have a SAM.gov Unique Entity ID (UEID).

Subcontractors and Supply Chain Risk Management Requirements

The Contractor shall not engage subcontractors or third parties with access to the Zero Trust Environment without prior written approval from APPA.

All subcontractors shall:

- Be subject to the same U.S.-based personnel restrictions as the Contractor.
- Inherit all applicable cybersecurity, zero trust, and compliance requirements.

The Contractor shall notify APPA promptly of any changes in personnel, subcontractors, or access that could impact compliance with this RFP.

Support Hours and Service Level Requirements

The Contractor shall provide operational and technical support for the secure Azure Government environment during standard business hours, defined as 9:00 AM to 5:00 PM Eastern Time, Monday through Friday, excluding federal holidays unless otherwise agreed in writing by APPA.

Support services during these hours shall include incident response, troubleshooting, security related support, configuration assistance, and coordination of remediation activities associated with the operation and maintenance of the environment.

The Contractor shall classify incidents based on severity and business impact and respond within the following timeframes during support hours:

- Critical incidents that result in a complete loss of service, a material security event, or an inability to access the environment shall receive an initial response within 30 minutes.
- High severity incidents that cause significant service degradation, impact security controls, or affect multiple users or critical functions shall receive an initial response within one hour.
- Medium severity incidents that cause limited disruption and allow operations to continue shall receive an initial response within one business day.
- Low severity incidents that have minimal operational impact shall receive an initial response within two business days.
- Response time is defined as the elapsed time between notification by APPA and acknowledgement by the Contractor.

The Contractor shall make reasonable efforts to resolve or mitigate incidents promptly following initial response. For critical and high severity incidents, the Contractor shall provide regular status updates during business hours until the issue is resolved or stabilized.

The Contractor shall maintain documented escalation procedures to ensure timely involvement of senior technical resources when incidents are not progressing toward resolution. Escalation procedures shall be provided to APPA and kept current throughout the period of performance.

The Contractor shall track service level performance and provide summary reporting as part of regular status updates to APPA. Repeated failure to meet service level requirements may be treated as a performance concern under the contract.

Service level requirements do not apply to issues caused by factors outside the Contractor’s reasonable control, including failures of third-party services.

Pricing and Cost Structure Requirements

Proposals must include a complete and transparent cost proposal that identifies all costs required to meet the requirements of this RFP, including platform licenses, subscriptions, services, implementation activities, and ongoing operational support.

Contractors must clearly identify the proposed pricing structure and align pricing to either a Firm Fixed Price model or a Time and Materials model. APPA may consider one or both pricing structures during evaluation.

Firm Fixed Price

Contractors proposing a Firm Fixed Price model must provide a fixed price, or fixed prices by phase, that include all costs necessary to deliver the required services and deliverables. This includes implementation, configuration, documentation, required platform and security tool licenses, and ongoing operational and support services for the defined contract period.

Firm Fixed Price proposals must clearly identify what is included in the fixed price and document any assumptions related to scope, usage, or scale. Costs not explicitly included in the Firm Fixed Price proposal may be deemed out of scope and may not be eligible for later reimbursement without prior written approval from APPA.

Time and Materials

Contractors proposing a Time and Materials model must provide detailed and transparent pricing that clearly distinguishes labor and non-labor costs. Proposals must include a labor rate card by role, estimated levels of effort by phase or activity, and itemized pricing for all required platform, security, monitoring, and management tool licenses and subscriptions.

Time and Materials proposals must include an estimated total cost or a not to exceed amount for implementation and for ongoing operations. APPA reserves the right to establish cost ceilings, approval thresholds, or spending limits for Time and Materials engagements.

License and Platform Cost Disclosure

Regardless of pricing structure, Contractors must explicitly disclose:

- All Microsoft Azure Government related costs required to support the proposed solution.
- All third-party licenses, subscriptions, or usage-based fees required to meet the requirements of this RFP.
- Whether licenses are proposed to be procured directly by APPA or through the Contractor.
- Any assumptions regarding consumption, scaling, renewals, or cost escalation.
- Failure to include pricing for required platform licenses or services may be considered a material omission.

Deliverables

The Contractor shall deliver the following deliverables over the lifecycle of the engagement. Deliverables are cumulative and must be maintained throughout the period of performance unless otherwise approved by APPA.

Phase 1: Project Initiation and Design

Target Completion Date: June 15

Deliverable 1.1: Project Kickoff and Implementation Plan
A documented implementation plan that includes project milestones, roles and responsibilities, communication cadence, risk management approach, and change control procedures.

Deliverable 1.2: Secure Azure Government Architecture Design
Detailed design documentation describing the Azure Government environment, including network segmentation, identity and access controls, endpoint security approach, logging and monitoring architecture, secure connectivity, and zero trust enforcement mechanisms.

Deliverable 1.3: Security Design Alignment Documentation
Documentation demonstrating alignment with APPA approved cybersecurity requirements and NIST SP 800-171.

Phase 2: Environment Build and Implementation

Target Completion Date: July 31

Deliverable 2.1: Azure Government Environment Implementation
A fully deployed and configured Azure Government environment, including cloud resources, networking, identity services, security tooling, monitoring capabilities, and secure connectivity.

Deliverable 2.2: Endpoint Configuration and Deployment
Configuration and deployment of two dedicated laptops, including device enrollment, encryption, application allow listing, centralized management, and enforcement of secure access controls.

Deliverable 2.3: Security Monitoring and Logging Enablement
Implementation of centralized security monitoring and logging, including log sources, alerting configurations, retention settings, and security dashboards.

Implementation Milestone Requirement
All implementation activities described in Phase 2 must be completed no later than July 31. Failure to meet this milestone may be considered a material performance issue.

Phase 3: Validation and Operational Readiness

Target Completion Date: August 31

Deliverable 3.1: Security Control Evidence Package
Audit ready documentation demonstrating effective implementation of required security controls, including configuration baselines, access controls, change records, and vulnerability remediation artifacts.

Deliverable 3.2: Incident Response and Operational Procedures
Documented incident response procedures, escalation paths, communication protocols, and recovery processes applicable to the environment.

Deliverable 3.3: Operational Runbooks
Operational runbooks documenting routine maintenance tasks, monitoring procedures, patching workflows, troubleshooting guidance, and support processes.

Phase 4: Operations and Ongoing Support

Period: September 1 through April 30, 2028

Deliverable 4.1: Ongoing Operations and Maintenance
Continuous operational support including monitoring, patch management, vulnerability remediation, configuration management, and incident response assistance.

Deliverable 4.2: Periodic Security and Compliance Updates
Updated security control evidence and documentation provided on a recurring basis or following material changes.

Deliverable 4.3: Status Reporting
Regular status reports summarizing operational health, security posture, incidents, risks, and planned changes.

Deliverable 4.4: Ongoing Compliance and Audit Support

The Contractor shall provide quarterly compliance self-assessment reports demonstrating continued alignment with NIST SP 800-171 and APPA-approved cybersecurity requirements.

The Contractor shall support APPA in responding to audits, reviews, or information requests from the Department of Energy or other authorized entities.

Phase 5: Contract Closeout and Transition

Target Completion Date: April 30, 2028

Deliverable 5.1: Final Documentation Package
A complete and current set of architecture documentation, configuration baselines, security control evidence, and operational runbooks reflecting the final state of the environment.

Deliverable 5.2: Transition and Knowledge Transfer Support
Support for transition activities as directed by APPA, including knowledge transfer sessions and documentation handoff.

Deliverable 5.3: Transition and Exit Plan

The Contractor shall develop and maintain a documented transition and exit plan to support orderly transfer of services at contract conclusion or termination.

The plan shall include:

- Knowledge transfer activities.
- Documentation handoff.
- Credential and access transition procedures.
- Support during transition to APPA or a successor provider.

Acceptance of Deliverables

All deliverables are subject to review and acceptance by APPA. Acceptance will be based on completeness, accuracy, alignment with approved requirements, and operational effectiveness.

Proposal Submission

Proposals must include an executive summary, detailed technical architecture, security and compliance approach, endpoint management strategy, operational support model, staffing plan, assumptions, detailed itemized list of entire technology stack and pricing.

Contractors must explicitly describe how NIST SP 800-171 controls will be implemented and maintained.

Contractors must describe how they ensure compliance with U.S.-based support personnel requirements, including staffing controls and access restrictions.

Proposals must be submitted electronically no later than 5:00 p.m. Eastern Time on April 15, 2026.

All proposals must be signed by an individual authorized to bind the proposing organization. Proposals submitted by facsimile will not be accepted.

Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- Demonstrated alignment with APPA's approved cybersecurity requirements and the requirements of NIST SP 800-171, including support for a zero-trust security model.
- Technical soundness, security, and appropriateness of the proposed Microsoft Azure Government (GCC High) architecture, including the ability to meet the required implementation timeline and support ongoing operations.
- Demonstrated experience designing, implementing, and supporting secure environments in regulated or high-risk contexts, particularly within Azure Government.
- Ability to provide secure, reliable, and compliant operational and security support using United States based personnel only, including adherence to defined support hours and service level expectations.
- Overall value, clarity, completeness, feasibility, and realism of the proposal, including the Contractor's approach to delivery, staffing, governance, and long-term support.
- Demonstrated experience implementing and operating Zero Trust environments with explicit control enforcement.
- Demonstrated experience supporting high-risk or federally funded cybersecurity programs.
- Demonstrated ability to provide long-term operational support with continuous compliance and audit readiness.

Terms And Conditions

Contract Term and Payment

The contract awarded under this Request for Proposal shall commence upon execution and shall conclude on April 30, 2028, unless otherwise terminated or extended in accordance with this RFP.

Payment for implementation related deliverables shall be processed on a Net 30 basis after APPA has reviewed, approved, and accepted the applicable deliverables in accordance with this RFP and the resulting contract.

Payments for ongoing operations, maintenance, and support shall be processed within thirty calendar days following APPA's receipt and approval of a properly submitted invoice.

No payment shall be made for work performed beyond the scope of the contract price unless such work is expressly authorized in writing by APPA.

The final payment schedule and invoicing structure are subject to negotiation between APPA and the selected Contractor and shall be based on agreed milestones and deliverables.

Allowable Costs and Federal Compliance

This project is funded through a Cooperative Agreement with the U.S. Department of Energy. The selected Contractor shall be responsible for ensuring that all work performed under the resulting contract complies with applicable federal requirements, including but not limited to 2 CFR Part 200 and 2 CFR Part 910, which are available at https://www.ecfr.gov/.

Acknowledgment of Federal Support

Any publication, presentation, or publicly released material developed under this project, whether copyrighted or not, must include the following acknowledgment and disclaimer:

Acknowledgment:

"This material is based upon work supported by the Department of Energy under Award Number DE-CR0000026."

Disclaimer:

"This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."

Termination

Either party may terminate the contract upon thirty calendar days written notice. In the event of termination, all materials, documentation, work products, data, and work in progress generated under the contract shall be promptly delivered to APPA.

Reservation of Rights

APPA reserves the right to cancel or withdraw this RFP, in whole or in part, at any time prior to the award of a contract.

Issuance of this RFP does not obligate APPA to award a contract or to take any action suggested in any proposal.

Public Communications

News releases or public announcements pertaining to the selection of the Contractor or the work performed under this RFP shall not be made without prior written approval from APPA.

Proposal Submission and Communications

Proposals must be submitted electronically no later than 5:00 p.m. Eastern Time on April 15, 2026.

All proposals must be signed by an individual authorized to bind the proposing organization. Proposals submitted by facsimile will not be accepted.

Prior to proposal submission, all communications related to this RFP must be directed to rfp@publicpower.org via email. APPA will issue written addenda if clarification is required. No oral interpretations shall be considered binding.

APPA reserves the right to reject any or all proposals and to request additional information or clarification from respondents at any time during the evaluation process. All work performed under this engagement will be subject to APPA's contractual terms and conditions and any applicable program or organizational requirements. The selected Contractor shall be required to execute confidentiality, and non-disclosure agreements prior to the commencement of work.

APPA will notify all Contractors of the final selection decision by April 30, 2026. All proposal materials will be treated as confidential to the extent permitted by law.

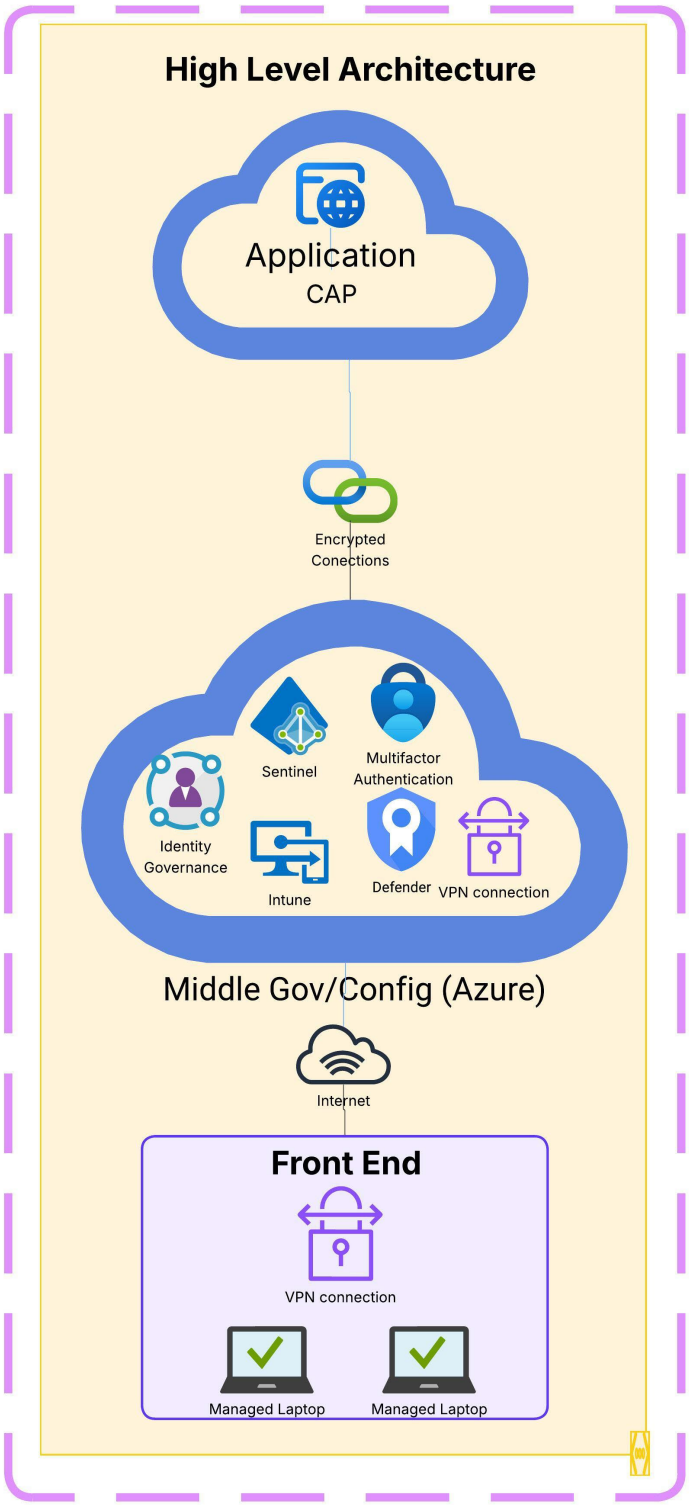
RFP Schedule

- April 2, 2026: RFP released
- April 16, 2026: Deadline for proposal submission

Primary Point of Contact

Lumi Kojcini
Senior Director, Information Technology
American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, Virginia 22202
Email: rfp@publicpower.org

Appendix A: High Level Architecture of ZTE environment



Appendix B: Sample Contract

AMERICAN PUBLIC POWER ASSOCIATION

SERVICES AGREEMENT

This Services Agreement ("Agreement") is made as the date of last signature below ("Effective Date"), by and between the American Public Power Association, at the address of 2451 Crystal Drive, Suite 1000, Arlington, VA 22202 ("APPA"), and _____, at the address of _____ ("Contractor"), for mutual consideration, the receipt and adequacy of which are acknowledged by the parties, who agree as follows:

1. **Object and Scope of the Agreement.** Contractor shall provide to APPA the services ("Services") as described in each Statement of Work ("SOW") attached hereto, or otherwise executed by the parties, and incorporated by reference. Contractor represents and warrants that the Services will be provided in a professional, competent, and timely manner, and in accordance with all applicable laws and regulations, and commensurate with industry standards.

2. **Statements of Work (SOWs).**
    a. Any SOW shall (i) describe the work to be performed; (ii) establish periods of performance; (iii) specify end-items to be delivered, if any; (iv) set forth schedules as required; and (v) provide pricing for the work.
    b. Except as otherwise stated in this Agreement, APPA shall have no financial obligation to Contractor that is not set forth in an SOW. Contractor shall not exceed dollar limits established in any SOW without prior written authorization from APPA.
    c. Any substantial change to an SOW, including but not limited to change in key personnel or change to timeline, must be approved in advance in writing by APPA.
    d. SOWs describing the Services, deliverables, timelines, and pricing shall be included or attached hereto, or incorporated by reference.

3. **Invoice Submission and Payment.** Contractor will issue invoices to APPA when each payment is due. The invoices will specifically detail what portions of the Services have been performed such that payment is due and will detail all out-of-pocket expenditures of Contractor for which reimbursement is sought from APPA with no markup above cost. Undisputed invoices will be paid by APPA within thirty (30) days of invoice receipt unless otherwise provided in the applicable SOW. Any invoiced amounts disputed in good faith shall not be due and payable until resolved.

4. **Relationship of the Parties.** Contractor is an independent Contractor, and nothing in this Agreement shall create an agency, partnership, employment, or joint venture relationship between APPA and the Contractor or any employees or agents of Contractor. Contractor will use independent judgment in completing the Services, will not be subject to APPA's day-to-

day supervision or control, will use the Contractor's own equipment and facilities, and will otherwise avoid aspects of employment inconsistent with independent Contractor status. Contractor will have sole and exclusive authority and responsibility for all of Contractor's employees and agents, and will be solely responsible for all taxes, insurance, and benefits except as otherwise agreed in writing to be paid or reimbursed by APPA.

5. **Intellectual Property.**

Each party's name, trademarks, pre-existing works or materials, and other intellectual property shall remain the property of the respective party, and shall be used by the other party only in performance of this Agreement or as otherwise authorized in writing by the respective party. All materials, content, data, or deliverables created or produced by Contractor within the scope of this Agreement ("Work Product") shall be deemed works made for hire and the property of APPA. To the extent that any Work Product may not, by operation of law, be work made for hire, Contractor by this Agreement irrevocably assigns, transfers, and conveys to APPA all right, title, and interest in and to such Work Product, and agrees to give APPA or its designees all assistance reasonably required to perfect such rights.

6. Confidentiality.

a. Contractor acknowledges that it may be exposed to certain information, documents, materials, plans, and/or property related to APPA or its activities, and affiliated groups and their activities ("APPA Materials"), that may be considered confidential or proprietary, including but not limited to financial information, member information, trade secrets, data, intellectual property, or other information ("Confidential Information"). Contractor agrees not to use or disclose, or to cause or allow to be used or disclosed, at any time during or after the term of this Agreement, any Confidential Information of APPA or others, except as specifically provided for in this Agreement or as otherwise specifically authorized in writing by APPA or the owner of such Confidential Information, and to return, delete, or destroy (at APPA's option) all such APPA Materials and Confidential Information upon termination or expiration of the Agreement. For the avoidance of doubt, Confidential Information does not include information rightfully disclosed to the Contractor by a third party with no obligation of confidentiality, or that is or becomes available from public sources through no wrongful act of the Contractor.

b. Contractor acknowledges that any breach of these obligations of confidentiality may result in immediate and irreparable damage to APPA and its affiliates, therefore APPA shall be entitled to seek from any court of competent jurisdiction preliminary and permanent injunctive relief and an accounting of all profits and benefits arising out of such violation, which rights and remedies shall be cumulative and in addition to any other rights or remedies to which APPA may be entitled. Contractor shall be responsible for any and every violation of these confidentiality provisions by its shareholders, directors, officers, employees, agents, advisors, and/or affiliates.

c. Contractor acknowledges and APPA agrees that Contractor may disclose Confidential Information in confidence directly or indirectly to federal, state, or local government officials, including but not limited to the Department of Justice, the Securities and

Exchange Commission, the Congress, and any agency Inspector General or to an attorney, for the sole purpose of reporting or investigating a suspected violation of law or regulation or making other disclosures that are protected under the whistleblower provisions of state or federal laws or regulations. Contractor may also disclose Confidential Information in a document filed in a lawsuit or other proceeding, but only if the filing is made under seal. Nothing in this Agreement is intended to conflict with federal law protecting confidential disclosures of a trade secret to the government or in a court filing, 18 U.S.C. § 1833(b), or to create liability for disclosures of Confidential Information that are expressly allowed by 18 U.S.C. § 1833(b).

7. **Term and Termination.**
   a. Term. The term of this Agreement shall begin as of the Effective Date and shall continue until completion of all applicable Statements of Work.
   b. Termination. Either party may terminate the Agreement and/or any SOW prior to the end of the term by written notice for material breach of the other party that remains uncured fifteen (15) days after notice of such breach is given. In addition, APPA may terminate the Agreement at any time for any or no reason, upon written notice to Contractor.
   c. Force Majeure. The performance of this Agreement by either party is subject to acts of God, war, government regulation, disaster, fire, epidemic, threatened or imminent strikes, civil disorder, curtailment of transportation facilities, threats or terrorist attacks, or other occurrence beyond the reasonable control of the parties, preventing or unreasonably delaying the performance of this Agreement. This Agreement may be terminated, or performance may be excused without penalty for any one or more of such reasons by written notice from one party to the other.
   d. Effect of Termination. Upon expiration or termination of this Agreement, Contractor shall return, delete, or destroy (at APPA's option) any APPA Materials or Confidential Information of APPA in its possession. The Contractor shall also provide to APPA all incomplete work or work in progress that was intended to be delivered as part of any SOW. APPA shall pay Contractor for the Services completed up to the date of termination, and any prepaid amounts not incurred shall be refunded to APPA within 30 days.

8. **Indemnification and Insurance.** Contractor shall indemnify, defend, and hold harmless APPA, its officers, directors, employees, and agents, from and against any and all suits, claims, damages, losses, liabilities, or costs, including reasonable attorneys' fees, resulting from the negligence, intentional misconduct, or breach of this Agreement by Contractor or its officers, directors, employees, or agents. Contractor shall maintain appropriate and sufficient insurance to cover its obligations under this Agreement.

9. **Miscellaneous.** This Agreement constitutes the entire agreement between the parties regarding its subject matter, and supersedes all prior writings or oral agreements. This Agreement may be amended only by a writing clearly setting forth the amendments and signed by the parties. Either party's waiver of or failure to exercise any right provided for in this Agreement shall not be deemed a waiver of any further or future right under this

Agreement. If any feature or provision of this Agreement is determined by a court of competent jurisdiction to be void or unenforceable, the balance of the Agreement shall survive and remain in effect. The provisions of this Agreement pertaining to Intellectual Property, Confidentiality, Indemnification, and such other provisions as by their nature should survive, shall survive the expiration or termination of this Agreement. This Agreement is binding on the parties, their successors and assigns, provided that no party may assign this Agreement without the prior written consent of the other party. All notices required or permitted under this Agreement shall be in writing and sent to the addresses in the preamble of this Agreement, or such other addresses as are designated by the parties by notice. This Agreement shall be governed by and interpreted in accordance with the laws of the Commonwealth of Virginia.

10. **Cooperative Agreement Specific Clauses**

All relevant requirements of the APPA/DOE Cooperative Agreement [Agreement] dated [Date], including the requirements outlined in 2 C.F.R. part 200 and 2 CFR Part 200 Appendix II, as modified by 2 C.F.R. 910, shall be incorporated into this Agreement by reference.

Contractor shall provide APPA confirmation of Contractor's registration and active status in SAM.

Contractor shall execute a Non-Disclosure Agreement consistent with the Non-Disclosure Agreement Template in Appendix C.

APPA may terminate this Agreement for convenience if it believes, in its sole discretion that it is in the best interest of APPA to do so, by providing thirty (30) day advance written notice to Contractor according to the procedures established in this Agreement.

Contractor will not and has not used federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any federal contract, grant or any other award covered by 31 U.S.C. 1352.

As appropriate and to the extent consistent with law, Contractor should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

If the Contractor (including any of its subrecipients and Contractors) anticipates involving foreign nationals in the performance of this award, APPA will be required to provide the Department of Energy (DOE) with specific information about each foreign national to satisfy requirements for foreign national participation. A "foreign national" is defined as any person who is not a United States citizen by birth or naturalization. The volume and

type of information collected may depend on various factors associated with the award. DOE concurrence may be required before a foreign national can participate in the performance of any work under this Agreement. Approval for foreign nationals from countries identified on the U.S. Department of State's list of State Sponsors of Terrorism must be obtained from DOE before they can participate in the performance of any work under this Agreement. Contractor must include this term in any in any applicable sub contractual agreement(s) associated with this Agreement.

Invoices shall have:

Bill to: APPA as addressee

Contractor name

Contractor address

Unique contract identifier

DOE Cooperative Agreement number: DE-CR0000026

DOE Cooperative Agreement Task number: [number]

Contractor Agreement amount

Contractor Agreement duration (MM/YY – MM/YY)

Total contract to date invoiced amount

Current invoice number

Invoice amount

Period services were rendered

Detailed list of charges

Contractor(s) shall include the proper citation for any sharing of data or reporting that contains the following:

Acknowledgment: "This material is based upon work supported by the Department of Energy under Award Number(s) [Agreement]."

Disclaimer: "This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express

or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."

Nothing in this Subaward or any Exhibits hereto shall be construed to: (i) to abrogate the full scope of the limits on DOE's liability available under all applicable law, or (ii) to constitute any agreement on behalf of DOE to any joint and several liability whatsoever.

Any notice, demand, or request provided for in this Subaward shall be in writing and shall be deemed properly served, given, or made if delivered in person or sent by courier service providing next-day delivery or sent by United States mail, registered or certified, postage paid, to the person and to the address specified below:

If to APPA: [name]

American Public Power Association

2451 Crystal Drive, Suite 1000, Arlington VA 22202

If to Contractor: [name]

[Address]

If sent by mail, notices shall be effective three (3) business days after deposit in the mail. If hand-delivered, notices shall be effective upon delivery. If sent by email and upon the receipt by the sending party of written confirmation by the receiving party. Either APPA or Contractor may, at any time, by notice to the other pursuant to this section, change the designation or address of the person specified as the one to receive notices.

APPA **Contractor**

Sign:_____ Sign:_____

Name: _____ Name: _____

Title: _____ Title: _____

Date: _____ Date: _____

Appendix C: Sample Non-Disclosure Agreement

APPA Non-Disclosure Agreement Cooperative Agreements

APPA Confidentiality and Nondisclosure Agreement

This Agreement is made and entered into as of _____, by and between the American Public Power Association ("APPA") and _____ ("Participant")

Confidentiality: Except as otherwise set forth herein, you agree that any American Public Power Association ("APPA") software, services, and/or hardware (including related documentation and materials) provided to you under this Agreement, and any information disclosed by APPA to you in connection with this Agreement will be considered and referred to as "APPA Confidential Information."

Notwithstanding the foregoing, APPA Confidential Information will not include: (a) information that is generally and legitimately available to the public through no fault or breach of yours; (b) information that is generally made available to the public by APPA; (c) information that is independently developed by you without the use of any APPA Confidential Information; (d) information that was rightfully obtained from a third party who had the right to transfer or disclose it to you without limitation; or (e) any third-party software and/or documentation provided to you by APPA and accompanied by licensing terms that do not impose confidentiality obligations on the use or disclosure of such software and/or documentation.

Sharing APPA Confidential Information: APPA wishes to share APPA Confidential Information under Cooperative Agreement Award Numbers: DE-CR0000026 (hereafter "CA") including all related materials with the Participant for the purpose of meeting the objectives of the CA and to review and assist with other work products specific to CA tasks for submission to the Department of Energy.

Nondisclosure and Nonuse of APPA Confidential Information: Unless otherwise expressly agreed or permitted in writing by APPA, you agree not to disclose, publish, or disseminate any APPA Confidential Information to anyone other than to employees and Contractors working for the same entity as you and then only to the extent that APPA does not otherwise prohibit such disclosure. You further agree to take reasonable precautions to prevent any unauthorized use, disclosure, publication, or dissemination of APPA Confidential Information. You acknowledge that unauthorized disclosure or use of APPA Confidential Information could cause irreparable harm and significant injury to APPA that may be difficult to ascertain. Accordingly, you agree that APPA will have the right to seek immediate injunctive relief to enforce your obligations

under this Agreement in addition to any other rights and remedies it may have. If you are required by law, regulation, or pursuant to the valid binding order of a court of competent jurisdiction to disclose APPA Confidential Information, you may make such disclosure notwithstanding anything else in this agreement, but only if you have notified APPA before making such disclosure and have used commercially reasonable efforts, to the extent permissible by governing law applicable to Participant to limit the disclosure and to seek confidential, protective treatment of such information. A disclosure pursuant to the previous sentence will not relieve you of your obligations to hold such information as APPA Confidential Information.

Removal of Participants: APPA, at its discretion, will remove any Participant from the CA program if the Participant willfully violates this Agreement.

Return or Destruction of Confidential Information: Promptly upon written request of APPA, the Receiving Party shall, and shall cause its Representatives to return to the Disclosing Party or destroy all Confidential Information in tangible form (whether in written form, electronically stored or otherwise), and neither the Receiving Party nor any of its Representatives shall retain any copies or extracts thereof.

Information Security: Without limiting Participant's obligation of confidentiality as further described in the Agreement and herein, Participant will be responsible for establishing and maintaining an information security program that is designed to: (i) ensure the security and confidentiality of APPA Data; (ii) protect against any anticipated threats or hazards to the security or integrity of the APPA Data; (iii) protect against unauthorized access to or use of the APPA Data; (iv) ensure the proper disposal of APAA Data; and (v) ensure that all subcontractors of Contractor, if any, comply with all of the foregoing.

Participant will designate an individual to be responsible for the information security program. Such individual will respond to APPA inquiries regarding computer security and to be responsible for notifying APPA-designated contact(s) if a breach occurs.

Upon becoming aware of a breach affecting APPA Data, Participant will immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof**.** Participant shall without undue delay (and in no event later than 72 hours of becoming aware of such breach) inform APPA and provide written details of the breach, including the type of data and systems affected, the likely consequences of the breach, any other relevant information for APPA to understand the nature of the breach, and the measures taken or proposed to be taken to address it, as soon as such information becomes known or available to Participant.

Participant agrees that any and all transmission or exchange of platform application data with APPA and other parties shall take place via secure means, e.g., HTTPS, FTPS, SFTP, or equivalent means.

DOE Required Assurances:

a. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive Order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this agreement and are controlling.

b. The limitation above shall not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

c. Notwithstanding provision listed in paragraph (a), a nondisclosure or confidentiality policy form or agreement that is to be executed by a person connected with the conduct of an intelligence or intelligence related activity, other than an employee or officer of the United States Government, may contain provisions appropriate to the particular activity for which such document is to be used. Such form or agreement shall, at a minimum, require that the person will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government. Such nondisclosure or confidentiality forms shall also make it clear that they do not bar disclosures to Congress, or to an authorized official of an executive agency or the Department of Justice, that are essential to reporting a substantial violation of law.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

APPA	Organization: [Name]
By: _____	By: _____
Date: _____	Date: _____