PROJECT REQUEST FOR QUALIFICATIONS ("RFQ")
CONSULTANT INSTRUCTIONS

RFQ Title: Cyber Security – 07 PSEGLI Vulnerability Assessment/Penetration Test
RFQ Title: Cyber Security
Released: 10/08/2025
Questions Due: 10/14/2025 @ 12 Noon
Due Date: 10/20/2025 @ 3 PM

Eligible Prime Proposers
Burns & McDonnell
Ernst & Young
Optic Cyber Solutions

In accordance with your firm's contract with the Long Island Power Authority (PSEGLI or the Authority), your firm is invited to submit a quotation for the above-stated project in accordance with the requirements of the attached Project Request for Qualifications-Scope of Work ("SOW") document.

Please use the attached Project Request for Qualifications Requirements to provide your firm's response.

LIPA's contact person for this project is Rosa Rhoden**, Manager of Procurement.** The due date and time for receipt of responses to this Project RFQ is indicated above.

Submission:

Long Island Power Authority (LIPA) has implemented a new e-Procurement platform called Bonfire. All RFQ submissions must be uploaded electronically to https://lipower.bonfirehub.com . Late proposals will not be accepted, nor will additional time be granted to any individual Contractor.

For a quick tutorial on how to upload a submittal, visit:

Vendor Registration and Submission

Addenda:

If, at any time, LIPA changes, revises, deletes, clarifies, increases or otherwise modifies this RFQ, LIPA will issue a written Addendum to the RFQ, which will be uploaded to the Bonfire portal.

Questions shall be submitted in writing using the Bonfire platform no later than the written questions deadline. Questions submitted after the deadline may not be answered. Proposers should rely only on written statements issued through the Bonfire platform.

The list of questions received with answers will be provided to all consulting firms who have been solicited via this Project RFQ via Bonfire.

PSEGLI will not accept quotations received after the due date. PSEGLI reserves the right to reject quotations that are incomplete.

This project will be performed on the basis of Fixed Price (Not to exceed amount) based on hourly rates from master contracts.

No work is authorized to commence without written authorization from the responsible LIPA Department Head. The Department Head responsible for the Project RFQ is Greg Flay, Chief Information Officer.

PSEGLI Vulnerability Assessment and Penetration Testing

Statement of Work and Proposal Requirements

Final Version

Oct-25

Contents

Introduction

LIPA's oversight of PSEGLI requires that information systems supporting its mission be assessed on an annual basis. Recognizing the importance of information systems, Lipa's Board has adopted an Information Technology and Cyber Security policy to support LIPA's vision.

To comply with this board policy, LIPA is requesting quotations from qualified cybersecurity vendors to conduct a comprehensive penetration testing assessment of PSEGLI's Enterprise and Operational Technology (OT) environments. The objective of this engagement is to identify vulnerabilities, assess risks, and provide actionable recommendations to strengthen our cybersecurity posture.

Objectives

The third-party vendor will conduct a comprehensive review of PSEGLI's IT and OT environments, identify potential vulnerabilities and misconfigurations in systems and network devices, and provide recommendations to remediate these findings.

Scope Of Work

Please note that for both IT and OT systems in scope, PSEG-LI maintains a primary and a secondary (used for disaster recovery) site and the scope described below includes systems and applications located at both these sites.

The selected vendor will provide penetration testing services that include, but are not limited to:

a. External Network Penetration Test

- Assess public-facing systems and services hosted on-prem and on the cloud.
- Identify vulnerabilities exploitable from the internet.
- Attempt controlled exploitation to validate risk.
- Testing will be performed during business hours (Eastern Time).

- Scope includes up to 100 IPs and a single principal DNS domain.
- Engagement will be conducted remotely.
- Client may provide valid accounts to test security controls such as MFA, authentication, and network porosity.
- PSEGLI will provide the address of the system(s) in scope prior to the engagement.

- Testing will simulate an opportunistic external attacker using vulnerability assessments, scanning, and targeted exploitation of high-risk hosts.
- Vendor will use best efforts but cannot guarantee identification of all vulnerabilities within the engagement timeframe.
- Testing will be conducted overtly, and security devices (firewalls, IPS, SIEM) may generate alerts during testing.

b. Internal Network Penetration Test

- Simulate an attacker with internal network access.
- Test segmentation between corporate IT and OT networks.
- Evaluate Active Directory and identity management security.
- Testing will be performed during business hours (Eastern Time).
- Scope includes more than 1,000 active IPs, primarily Windows-based assets. All assets and VLANs are accessible via a single site.
- Testing may be conducted remotely using a vendor-provided virtual machine (VM) deployed in bridged mode, capable of seeing the internal network as any workstation.
- The VM should be placed on a subnetwork where targeted assets are reachable and where active user traffic exists.
- For passive listening, a NIC will be provided per VLAN being tested.
- The VM must not be tampered with, as this may disable protection mechanisms or invalidate test results.
- Client may provide a valid domain account depending on threat model. If no credentials are provided at the start, testers may request them later.
- Testing will be conducted overtly, and security monitoring systems may generate alerts.

c. Wireless Network Penetration Testing

- Testing will be performed during business hours (Eastern Time).
- Scope includes 1 location with 2 SSIDs.
- Engagement may be performed remotely using a portable Wi-Fi testing appliance shipped to PSEG-LI by the vendor.
    - The appliance must be deployed by PSEG-LI prior to start of testing.
    - A PSEGLI technical point-of-contact will position the device near wireless users to simulate interception-based attacks.
    - If physical positioning is not feasible, the point-of-contact may be asked to connect to the SSID to generate traffic.
- PSEG-LI shall not tamper with the virtual machine/appliance provided since it could disable some built-in protection mechanisms and lead to potential impact on the tested environment.

- The vendor may request wireless credentials to test certain aspects of a specific network (e.g. network segregation) if compromise is not achieved.
- The testing will be conducted overtly. PSEG-LI should be informed that security devices / Firewalls / Wireless IPS alerts might be generated during testing.

d. Web Application Testing

- Conduct OWASP Top 10-based testing on critical web applications (customer portals, billing systems, SCADA web interfaces, if applicable).

e. Operational Technology (OT) Security Assessment

- Review ICS/SCADA systems for exposure and vulnerabilities.
- Validate network isolation and remote access controls.
- Conduct non-disruptive testing in coordination with operations staff.
    - Work on some OT systems will require NERC CIP authorization and training.

Schedule of Key Deliverables

1. Project Management Plan (due two weeks after Notice to Proceed)
2. Weekly Status Report (due by COB each Friday for Tuesday morning virtual/in-person review meeting)
3. Draft Assessment Report (due eight weeks after Notice to Proceed)
4. Draft Recommendations Report (due 12 weeks after Notice to Proceed)
5. Draft Integrated Final Report (Narrative format) and Draft Management Read Out (presentation format) (due 16 weeks after Notice to Proceed)
6. Integrated Final Report and Management Read Out (due 18 weeks after Notice to Proceed)

Project Deliverables

- Executive summary (non-technical) for leadership.
- Technical report detailing findings, risk ratings, and remediation recommendations.
- Presentation and walkthrough of results with IT and OT leadership teams.

Project Management Plan

This deliverable will describe the following:

1. The consultant's overall technical approach to executing the project's defined scope and developing the project's key deliverables.
2. The consultant's resource plan.
3. Detailed project schedule that will be used to baseline the overall project schedule performance.

Final Report

The report will provide a high-level overview of the assessment process, the methodology followed, recommendations, and overall implementation plan, including the following:

1. The objectives and overall approach followed
2. The scope of the assessment includes:

    a. Information technology environment
    b. Cyber security standards, tools, methods, and guidelines
    c. The evaluation approach used to identify the current cyber security posture

    The information technology environment (IT) scope encompasses all systems and assets, regulations or requirements, and the identified risks and threats to the systems.

3. The detailed overview of assessment results and the methodology followed
4. Description of the strategic recommendations and key areas of focus for remediation
5. Detail information on the pentation testing and configuration review results and recommendations
6. Provide an overall roadmap, plan, and timeline of the path towards remediating the major findings

Assessment Report

The assessment report will include the following:

- Assess and document the current state and security posture of PSEGLI's IT environment
- Identify the gaps, vulnerabilities, and misconfigurations, ranking their severity and priority.
- Describe and create a plan of actionable and prioritized mitigation actions to close the gaps based on available resources, business needs, and current cyber security risk environment—to achieve the desired cyber security posture.
- Document results in a tabular format, including the current state, target state, and gaps, and prioritize mitigation actions.

Penetration Testing and Configuration Assessment

Perform an external network (Internet) assessment and identify vulnerabilities on PSEGLI's hosts visible from the Internet. Scan IP address ranges to identify live hosts, services running on the live hosts, and potential known vulnerabilities associated with the services. Manually validate the identified vulnerabilities. The vendor will work with the PSEG-LI Cyber Security Team to determine which hosts are to be evaluated and to define any exclusions.

Assess the internal network, including servers, workstations, and other network devices accessible through the internal environment. Assess with the objective of gaining access to sensitive information without any knowledge of the internal network infrastructure map, identifying vulnerabilities and escalating privileges with only an Ethernet connection on-site. Where an on-site Ethernet connection is required, details such as asset registration, rogue device discovery implications, and whether vendor devices will be added as known assets will be worked out and agreed upon during the Rules of Engagement (ROE) sessions with PSEG-LI.

Perform a configuration review of PSEGLI's hosts and network devices to determine configuration anomalies and issues. Utilize industry-standard benchmarks to compare the configurations for each host and network device with any high-risk designs. (e.g. CIS-CAT)

All testing should be conducted in a passive manner to avoid unnecessary disruptions to the production environment and coordinated with PSEGLI's Cyber Security Team.

Recommendation's Report

This report will include details of actionable recommendations implementable within the Implementation Period, including:

- Provide an estimated cost and/or effort for each of the various corrective controls that can be implemented to achieve the desired state
- Provide different approaches to corrective controls that may result in faster implementation or reduction in overall cost
- Propose a roadmap and develop a project plan and timeline for implementing all the recommendations. Provide concrete metrics that can be used to monitor and measure each of the implementation steps. Describe the end-state achieved upon successfully completing each "cyber security remediation program" implementation step within the implementation period.

Penetration Testing and Configuration Assessment

Develop recommendations based on the penetration test and configuration review assessment findings to remediate the identified security risks.

Terms and Conditions

- Testing must be conducted in a non-disruptive manner, with pre-approved scheduling.
- Vendor must sign a Non-Disclosure Agreement (NDA).
- Vendor must comply with all applicable laws, regulations, and industry standards.
- All findings and reports are the sole property of The Long Island Power Authority**.**

Management Read Out

The Management Read Out is an executive-level presentation developed by the Consultant and will describe/discuss, at a minimum, the following topics:

- Project Objectives
- Executive Summary
- Technical Approach for Assessment and Findings
- Key Findings and Risk Elements
- Methodology for Development of Recommendations
- Methodology for Prioritization of Recommendations
- Proposed Implementation Timeline
- Discussion of Cost Estimates for Implementation
- Penetration Testing and Configuration Review Results and Recommendations
- Next Steps for PSEGLI

The Management Read Out should not exceed 50 pages.

> ***Report-type deliverables must document all the steps and details of the assessment process, results, and recommendations in MS Word. Presentation format reports must be delivered in MS PowerPoint format.***

Proposal Requirements

Consultant's Technical Proposal will provide the following:

1. Consultant's overall technical approach to executing the project's defined scope and developing the project's key deliverables.
2. Consultant's resource plan that identifies consultant's personnel to be engaged in the project, short description of their expected role on the project, their "labor category" consistent with those described in the master contract, the period of their engagement in the project relative to the project timeline and resumes for each of the proposed consultants.
3. Confirmation of security and background checks. Information related to past in-active or active security clearances.
4. Proposed project timeline.
5. Any consultant assumptions used to develop the proposal.
6. PSEGLI may request names and addresses of up to 3 references for vendor engagements of a similar nature.
7. The length of the proposal should be limited to 25 pages, excluding resumes.

Frequently Asked Questions

1. Question: What level of detail is required for the recommendations?

   Answer: Recommendations will describe specific controls that will improve the cyber security posture. The recommendations should clarify the control objective, potential technical approaches to implementation, estimated time for completion, and estimated internal and external costs to implement. POAM (see NIST SP 800-37) level detail will not generally be required, but there should be enough substance in the recommendation such that robust POAMs can be constructed from the recommendations. We want a set of controls that can reasonably be implemented during the implementation period with estimated costs to execute the recommended actions.

2. Question: What type of cost estimates are needed for Recommendations?

   Answer: Estimated cost can be in rough order of magnitude or based on consultants' best judgment and experience. In the case of rough order of magnitude estimates, provide the basis for estimation. Provide cost for labor, tools, or level of effort required for the configuration change.

3. Question: What details are expected in the Management Readout?

   Answer: The Management Readout will be detailed and address the management overview and the technical details. For further guidance, refer to the outline provided in the Management Readout section.

4. Question: Are any specific security credentials required for personnel working on this project?

   Answer: Contractor personnel is expected to be US citizens and US residents and will be required to undergo PSEGLI prescribed security screening (e.g., background checks, drug screening, etc.). If proposed personnel have current or past US Government security clearances, please indicate that in the resumes of the personnel proposed.

5. Question: Are there any specific data protection requirements for the information shared?

   Answer: The consultant will reasonably protect all information shared during this project and comply with all the laws and regulations; we will set up a shared and protected environment during this engagement.

6. Question: What are the evaluation factors?

   Answer: The evaluation factors are 40% technical proposal, 30% technical team (personnel), and 30% cost.

7. Question: Is formal benchmarking with other utilities included in the scope?

   Answer: Benchmarking is not included in the scope of this project.

8. Question: When do you expect to issue the Notice to Proceed (NTP)?

   Answer: We expect to issue the NTP shortly.