TENDER DOCUMENT

FOR

Operational Technology Cybersecurity Assessment

Prepared by:
Belize Electricity Limited
Telecommunications Department
2½ Miles Philip Goldson Highway
Belize City, Belize
February 2024

Bidders will be required to submit proposals via email to bidsubmittal@bel.com.bz no later than **3:00 p.m. on Friday, March 29, 2024,** and labeled:

BID #2024-2313 Operational Technology Cybersecurity Assessment

IMPORTANT DATES:

- Expression of Interest for virtual pre-bid meeting must be submitted via email to bidboxrequest@bel.com.bz no later than 3:00 p.m. on Wednesday, March 20, 2024.
- Virtual pre-bid meeting – Friday, March 22, 2024.
- Bid due date – 3:00 p.m. on Friday, March 29, 2024.

GENERAL

1. Terms and Definitions

Abbreviation:	Description:
BEL	Belize Electricity Limited
IoCs	Indicators of Compromise
OT	Operational Technology
IT	Information Technology
ICS	Industry Control Systems
IPP	Independent Power Producer

2. Company Overview

BEL is the primary distributor of electricity in Belize. The Company owns and operates a national electricity grid, which connects all major municipalities using 1900 miles of transmission and primary distribution lines. The grid is supplied by local IPPs utilizing hydroelectricity, biomass, petroleum and solar energy sources; and is secured and stabilized by a 115- kV interconnection with Mexico. A team of operations engineers and technicians and control center operators utilize a host of hardware and software systems and devices, within the OT network, to gather real-time data from remote locations and devices to monitor and control the grid and to analyze related processes.

OBJECTIVES, SCOPE, AND ASSUMPTIONS

3. Objectives

There are two key objectives of this engagement:

I. To understand the extent to which the OT environment at BEL may have, or potentially could have been, breached from a cybersecurity perspective, with advice on how to remediate any issues identified within the OT environment.

II. To evaluate the overall risk posture of the OT environment that could be affected by a cyber-attack and provide a strategic roadmap for improving the security posture of the OT infrastructure and reduce the risk of cyber-attacks in line with BEL's risk tolerances/appetite.

4. Scope & Assumptions

The consultant will perform the following scope of works to achieve the broad-based objectives.

4.1. Threat Hunt

Threat Hunt proactively searches for adversary activity within the predetermined networks, systems, or assets identified during the scoping effort. The Consultant will use their industry-leading knowledge of ICS-focused adversaries and their tactics, techniques, and procedures (TTPs) to provide real-world context to findings. The Consultant will leverage network diagram and documentation review, threat modeling, and data analysis to evaluate if there are indications of adversary activity in the client environment.

4.1.1. Scope

The service should allow for deep dive inspections into multiple hypotheses, using multiple data sources, related to a suspected breach. The engagement should incorporate the use of BEL's existing EDR, SIEM and vulnerability platforms where applicable and/or any other similar platforms, tools, raw packet captures, as well as Windows Event Logs, Historian data, and raw memory images, (where available, transferrable, and relevant). Hypotheses should be developed based upon an initial discussion with stakeholders and subject matter experts (for instance, OT personnel, network engineering, site IT, or vendors). This engagement can be done remotely or onsite.

4.1.2. Assumptions

For the Threat Hunt, Client will make available the following:

- Network Diagrams
- Packet Captures of ICS/OT ingress, egress, and core lateral movement locations
- IP Schema
- Zone and Conduit Assignments (where available)
- Asset Inventory (where available)
- Firewall Rules (where available)

4.2. OT Cybersecurity Assessment

The Consultant's OT Cybersecurity Assessment should focus on gathering a preliminary understanding of the existing network and security posture in relation to protection, detection, and response capabilities. Through documentation review and staff interviews, prioritized tactical and strategic recommendations are to be provided to strengthen the organization's ability to defend the critical industrial control systems.

4.2.1. Scope

Compromise Assessment

A Compromise Assessment (CA) should utilize BEL's existing security technologies and any other relevant network analysis tools to capture and inspect traffic samples looking for vulnerabilities in the Client's environments. As an outcome the Consultant will provide recommendations in network architecture to eliminate and/or reduce vulnerabilities to improve security posture, aligned with MITRE ATT&CK, IEC 62443, NIST CSF.

Topology Review

A Topology Review (TR) is a technical review of the Client's industrial network segment(s) to identify cybersecurity shortcomings. Network design is evaluated for security gaps, and recommendations are generated to strengthen the architecture and network systems.

Program Review

A Program Review is a review of the Client's policies, procedures, and organizational structure surrounding network security. Critical roles, responsibilities, approvals, and accountabilities are evaluated to identify potential improvements in defensibility. Corporate and site plans, such as Disaster Recovery, Incident Response, Business Continuity, and Risk Management shall be evaluated for corporate headquarters against individual site(s) for constancy and completeness.

Crown Jewel Analysis (CJA)

A Crown Jewel Analysis identifies primary assets and network locations where process disruption is most impactful to the Client. The Consultant shall work closely with the Client to identify points of maximum financial, operational, and business impacts through consequence analysis. The method to identify these Crown Jewels and process of analysis are to be described in the final report.

Collection Management Framework (CMF)

A Collection Management Framework is a process that documents and institutionalizes data sources that are available to defenders, including what information is available, where that data lives, how it is accessed, and how long that data is retained. Network diagrams, documentation, and staff interviews are to be used to develop a preliminary understanding of data locations and workflows across the network. An introductory CMF specific to the Client's environment is to be generated in coordination with the Client. The Consultant shall focus on knowledge transfer during CMF development and provide a roadmap that includes recommended actions to continue.

Sensor Placement Study (SPS)

Using information gathered during the CA and TR, the Consultant shall determine the optimal sensor type and placement for the Client's Cybersecurity Monitoring Platform. The final report will include an overview of the network topology and location of each sensor.

4.2.2. **Assumptions**

The Consultant can make several assumptions regarding the Client's responsibilities that can influence the success and timely completion of this engagement. The Consultant should make a formal Information Request at project initiation. The following high-level assumptions can be made for all engagements:

I. Client will designate a lead project liaison to help resolve issues related to this engagement.

II. Client will provide emergency security contacts; that is, information to be used in the event that urgent security vulnerabilities/issues are discovered.

III. Client will, at project initiation, provide access to all information and resources required to complete this engagement.

IV. Client will provide Network diagrams, inventory, device models, device firmware images, or any other artifacts required to complete the assessment.

V. Client will provide access to appropriate staff as needed during the engagement.

VI. Client will provide RFI data within 10 business days.

VII. Client will comment on all deliverables within 5 business days.

VIII. For the Topology Review, Client will provide current network diagrams and asset information.

IX. For the Program Review, Client will provide any information related to policies, procedures, programs, and technologies that supports the protection of the network(s) in scope.

X. For the Crown Jewel Analysis (CJA), Client will provide any information related to the network(s) and process(es) in scope. Additional information related to operational contingencies and cost may be requested.

XI. For the Collection Management Framework (CMF), Client will provide any information related to current security controls supporting protection, detection, and response of the network(s) in scope.

XII. Client will provide any information related to network packets capture for segments and subsegments of the network(s) in scope.

XIII. The total file size of the network packet captures will not exceed 30GB.

4.3. OT Environment

Proponents should put forward a proposed piece of work based on the following information about the OT environment:

Site Description	Asset	Estimated Number of OT Assets	Descriptions (make / model / year of commission)
Control Centre Assets	Firewalls	2	Palo Alto
	Switches	3	Cisco & Arista
	Servers	45	Dell VM Hosts. Virtual machines running mix of Linux & Windows
	Endpoints	27	Windows
	Other:		
Substations Assets	Routers	0	
	Switches	25	Cisco & Arista
	RTUs / RTACs	25 /12	ACS / SEL
	PLCs	0	
	HMIs	18 (3)	PCs (HMI Vendors: ACS / SEL / Woodward)
	Meters	10	PQM (GE), SEL or Shark
	Reclosers	25	Eaton Cooper
Secondary Network Assets	RTUs		
	PLCs		
	Communication devices		
	Other:		

SUBMISSION, INQUIRIES, AND EVALUATION

5. Submission and Inquires

5.1. Submission

Bidders are required to fill out the bidding schedule and submit via email to bidsubmittal@bel.com.bz no later than **3:00 p.m. on Friday, March 29, 2024,** labelled:

E-mail subject:

"BID #2024-2313 – Operational Technology Cybersecurity Assessment"

5.2. Inquires

Inquiries related to this tender will be addressed in a virtual pre-bid meeting, which will be held on Friday, March 22, 2024. To express interest in attending this meeting please send an email to bidboxrequest@bel.com.bz no later than **3:00 p.m. on Wednesday, March 20, 2024.** While this meeting is not mandatory, we strongly urge you to attend.

E-mail subject:

"EOI BID #2024-2313 – Operational Technology Cybersecurity Assessment"

You will be provided with a link to attend a virtual pre-bid meeting scheduled for Friday, March 22, 2024, shortly after your expression of interest.

6. Eligibility

The eligibility criteria are the minimum criteria to which the Bidder should comply. Compliance to the eligibility criteria will allow participation to the RFP process.

The eligibility criteria applicable are:

6.1. Financial criteria:

Submission of the financial statements for the past two (2) years. BEL prefers to receive audited financial statements, however will allow submission of financial statements which have not yet been audited from the Bidders.

6.2. Technical criteria:

Bidders shall furnish documented evidence that they have completed contracts with similar scope within the past five (5) years within the European, Asian or the Americas region.

6.3. Insurance

The proponent should have the following coverage in place. Certificates of coverage for each should be included with the submission.

Policy Type	Limits of Liability (in $USD)
Commercial General Liability	Minimum limit $2,000,000 per occurrence & maximum deductible $5,000 property damage
Technology Errors and Omissions	Minimum limit $3,000,000
Cyber and Privacy Liability	Minimum limit $3,000,000

6.4. Minimum references:

Two (2) references of successfully completed projects with a comparable scope of works, during the last five (5) years.

6.5. Currency:

Proposals are to be denominated in Belizean Dollars or United States Dollars

7. Evaluation Criteria

The Evaluation Criteria includes elements which will determine the best value proposal for BEL. The evaluation criteria have been grouped into technical and procurement related categories:

7.1. Technical

Criteria #:	Description:	Weight:
A3	Relevant experience of the firm (2 References with similar scope)	10
B1	Key experts Qualification and Competence	25
B2	Thoroughness of the approach, methodology & deliverables	25
B3	Project duration	10
B4	Resource Level of Effort by Key Project Stage	20
B5	Additional value creators	10
	Total:	**100**

7.2. Cost

Criteria #:	Description:	Weight:
B6	Price	100

8. Process Schedule

BEL has planned the following milestones and their completion date:

Milestone:	Description:	Ready by:
1.	RFP publication date	Friday, March 1, 2024
2.	Q&A session (bidders seek clarifications from BEL)	Friday, March 22, 2024
3.	Proposal submission by bidders	Friday March 29, 2024 3:00 PM
4.	• Q&A session (BEL seeks clarifications from bidders)	Friday, April 5, 2024

	• Finalization of the Evaluation and Selection Process	
5.	Start contracting process and start project	Friday, April 12, 2024

APPENDIX

Appendix A: Form of Proposal Submission

Section	Description
A1	Letter of Introduction
A2	Organization Profile
A3	Reference Projects
B1	Project Personnel
B2	Project Approach, Methodology and Deliverables
B3	Project Duration
B4	Resource Level of Effort by Key Project Stage
B5	Additional Value Creators
B6	Cost

A1 – Letter of Introduction

Provide a brief description as a cover letter of the Proponent and its business. This should demonstrate the Proponent's knowledge and understanding of the background, objectives, and issues involved in the Work as well as intended deliverables.

A2 - Organization Profile

Legal Operation Name	
Parent Company Name (if applicable)	
Head office address	
Local address	
Organization website	
Nature of incorporation (Inc., Partnership etc.)	
State date of operations	
<Need to see relevant procurement policies from BEL to add things like insurance requirements, quality management requirements etc.>	Insurance requirements (Public liability/employers' liability) for in person Stipulate whether work should Consider the inclusion of cybersecurity / Errors/omissions policies.
Etc.	

A3 – Reference Projects

Reference Project 1

Project Context	Project Name	
	Name of Client Organization	
	Project Business Case	Objectives sought 1. A 2. B 3. C 4. D 5. etc
Scope	Describe the Scope of work	Brief Description Stage 1 Stage 2 Stage 3 Stage 4 Etc.
Schedule	Project Schedule	In Progress or Completed (please indicate)
	Duration of project (in weeks)	
	Date of contract award	
	Date of contract completion (indicate if still in progress)	
Price	Please indicate • Fixed Price • Time & Materials • Other	Initial Pricing Estimate Actual project price at completion
Reference	Contact Name	
	Contact Title	

	Contact Phone Number	
	Contact Email	
	Contact Role on referenced project	

Reference Project 2

Project Context	Project Name	
	Name of Client Organization	
	Project Business Case	Objectives sought 6. A 7. B 8. C 9. D 10. etc
Scope	Describe the Scope of work	Brief Description Stage 1 Stage 2 Stage 3 Stage 4 Etc.
Schedule	Project Schedule	In Progress or Completed (please indicate)
	Duration of project (in weeks)	
	Date of contract award	
	Date of contract completion (indicate if still in progress)	
Price	Please indicate	Initial Pricing Estimate

	• Fixed Price • Time & Materials • Other	Actual project price at completion
Reference	Contact Name	
	Contact Title	
	Contact Phone Number	
	Contact Email	
	Contact Role on referenced project	

B1 - Project Personnel

Roles/Personnel	Name	# of years' Experience	Relevant Project Experience	Qualifications and Professional Designations	Is Sub-contractor?*
Project Manager			A) Project A Experience B) Project B Experience C) Etc.		
Specialist 1					
Specialist 2					
Etc.					

The descriptions of the team members should demonstrate that the team has experience in the domain of Operational Technology within energy utilities and understands developments in the energy sector that influence the types of security technologies and best practices required to safeguard an electrical grid and its ancillary systems. If sub-contractors are expected to be engaged, please also outline the terms of liability distribution that would apply.

B2 – Project Approach, Methodology and Deliverables

Approach and Methodology

The Replaceable sample template below should be adapted to incorporate the following requirements:

- Preparation phase / mobilization phase
- Milestones, key activities and deliverables
- Meeting structures (when, who and type of meeting – daily standup – weekly update – steering committee meeting).
- Dependencies between activities and milestones.
- Interdependencies with other projects running at BEL (if applicable).

Replaceable sample template.

Scope Area	Stage	Description
Threat Hunt	Stage 1	
	Stage 2	
	Stage 3	
OT Cybersecurity Assessment	Stage 1	
	Stage 2	
	Stage 3	
	Etc.	

Risk Mitigation Strategy for OT environment.

Proponents should document the key safeguards they intend to adopt/use as part of their approach to minimize the risk of unplanned, operational outage.

Deliverables*

Scope Area	Deliverable Description	Format of Deliverable
Threat Hunt		Docx
OT Cybersecurity Assessment		

*Each deliverable should include the following sections:

- Executive summary
- Methodologies used for analysis
- Findings with severity assignment
- Prioritized list of recommendations to address associated findings

B3 – Project Duration

Scope Area	Stage	Start Date	End Date
Threat Hunt	Stage 1		
	Stage 2		
	Stage 3		
OT Cybersecurity Assessment	Stage 1		
	Stage 2		
	Stage 3		
	Etc.		

B4 – Resource Level of Effort by Key Project Stage

Indicate the percentage of full time equivalent loading percentages per role, per project stage based on a 40 hour work week e.g. for 20 hours per week use 50%

Scope Area	Project Stage	Role			
		Project Manager	Specialist 1	Specialist 2	Etc.
Threat Hunt	Stage 1		1%	90%	
	Stage 2		5%	90%	
	Stage 3		10%	90%	
OT Cybersecurity Assessment	Stage 1				
	Stage 2				
	Stage 3				
	Etc.				

The proponent should also address the following points in addition to completing the aforementioned table.

- The project team (both from the Bidder as well as the proposed roles from BEL).
- The project staffing model (both from the Bidder as well as the proposed roles from BEL).
- The project governance model (both from the Bidder as well as the proposed roles from BEL).
- The Risk Management process. Bidders are required to indicate and describe how their proposed governance model will ensure the engagement (including concerns and feedback) with all relevant stakeholders in an effective manner.

B5 - Additional Value Creators

<Proponent to add 1 page of detail max to provide additional value add insights and how they will be incorporated into the engagement>

B6 – Cost

Scope Area	Fixed Price (Use $US or $BD)	Invoice Timing (milestone/date)	Invoice payment terms
Threat Hunt			
OT Cybersecurity Assessment			
Total			

If the proponent is expecting to charge back expenses for on-site travel that they would like to include in their plan, an explanation with assumptions/travel policy should be included.