United States Energy Association Request for Proposals:
Bolstering Kazakhstan's National Security
Through Electricity Market Cybersecurity

QUESTIONS & RESPONSES
June 27, 2024

QUESTION: What are the preferred electronic formats for deliverables?

- **Agendas**
- **Reports**
- **Drawings/Diagrams**
- **Presentations**
- **Survey Results**

ANSWER: The preferred electronic formats for agendas and reports shall be MS Word; for presentations MS PowerPoint, for survey results either MS Word (for processed results) or MS Excel (for raw data). The format for drawings and diagrams will be addressed on a case-by-case basis.

QUESTION: Task 1. Is there a known scope of the C2M2 assessment? For example, market operations systems or corporate IT?
ANSWER: The C2M2 assessment should include both market operations systems and corporate IT.

QUESTION: Does Task 2 require an updated hardware and software asset inventory as a deliverable?
ANSWER: Yes.

QUESTION: Task 3. What is the scope of the risk assessment, does it include all information system assets of the organization or is there a specific system boundary?
ANSWER: The risk assessment shall include all information system assets.

QUESTION: Task 3. What is the scope of the vulnerability assessment, does it include all information system assets of the organization or is there a specific system boundary?
ANSWER: Same as above.

QUESTION: Task 3. Are the assets which are to be included in the vulnerability assessment IT systems or OT systems?
ANSWER: Today it is mainly IT infrastructure, but there are plans for OT infrastructure as well. In addition, KOREM does not have OT assets. However, it is possible that some OT systems may be included to analyze data related to electricity generation and consumption.

QUESTION: Does Task 3 require an updated hardware and software asset inventory as a deliverable?
ANSWER: Yes.

QUESTION: Task 3. Is the vulnerability assessment meant to be a technical assessment which includes scans of individual assets using vulnerability scanning tools and other security tools?
ANSWER: Yes.

QUESTION: If Task 3 includes a technical vulnerability assessment, will the tools scan the assets using authenticated scans or non-authenticated scans?
ANSWER: Our strong preference is to use both.

QUESTION: If Task 3 includes a technical vulnerability scan will the consultant be required to scan all assets in the system or is this task time bound? For instance 1 day for training and 3 days of assessment/scanning, regardless of how many assets are in the target system.
ANSWER: Scanning shall be scheduled after the close of trading, i.e. in the afternoon, except when KOREM conducts auction bidding which usually takes place at 2pm.

QUESTION: If Task 3 includes a technical vulnerability assessment, will the consultant provide the tools or will KOREM?
ANSWER: The consultant shall provide all the tools.

QUESTION: If Task 3 includes a technical vulnerability assessment, will the consultant be allowed to bring hardware and software and use it in KOREM's environment to provide the technical vulnerability assessment?
ANSWER: Yes, once the responsible KOREM personnel has been notified.

QUESTION: If Task 3 includes a technical vulnerability assessment, is KOREM willing to sign a waiver of liability for the consultant while performing the technical vulnerability assessment upon KOREM's request?
ANSWER: The consultant shall identify possible risks and, together with KOREM, determine the parameters of possible consequences when conducting the assessment.

QUESTION: Deliverable 6. We believe there is a typo in the deliverable 6 language, we assume the language is specifying that subtasks 2.1 - 2.6 are included, not 2.1 - 4.6. Please confirm.
ANSWER: Yes, Deliverable 6 should read as follows. "A detailed plan for assisting KOREM with developing a digital asset inventory, data architecture, and digital architecture. The plan shall include all subtasks listed under Task 2 (subtasks 2.1 through 2.6) with objectives, required actions, expected deliverables, and a list of supporting materials. The plan shall be submitted to USEA as a draft for comment no later than three weeks prior to the scheduled commencement of the activity." We apologize for the typo.

QUESTION: General: We request two weeks extension of the proposal submission deadline.
ANSWER: We are unable to grant this request. The proposal submission deadline will be extended only if we receive fewer than 3 valid proposals in response to this RFP.

QUESTION: Technical Requirements and Standards: Any specific standards that KOREM must adhere to for its cybersecurity systems?
ANSWER: First and foremost, the Resolution #832 of the Government of the Republic of Kazakhstan on Unified Requirements in the Field of Information and Communication Technologies

and Information Security, then the Law of the Republic of Kazakhstan #418-V "On Informatization," and, optionally, ISO 27001 Information Security Management System.

QUESTION: Technical Requirements and Standards: Are there any industry-specific regulations or compliance requirements that need to be considered?
ANSWER: Since KOREM only uses IT, the rules and requirements will be the same as in the previous response. There are no specific industry rules applicable to KOREM's operations.

QUESTION: Digital Energy Platform: Please share short description on KOREM Digital Energy Platform.
ANSWER: The platform is designed to collect and analyze information related to the entire electricity industry of Kazakhstan, including generation, consumption, tariffs by region, etc. The trading platform performs the functions of wholesale purchase of electricity sales in Kazakhstan and trading operations.

QUESTION: Digital Energy Platform: Is this an IT or OT infrastructure?
ANSWER: Today it is mainly IT infrastructure, but there are plans for OT infrastructure as well.

QUESTION: Digital Energy Platform: Does the digital asset inventory requirement is for both IT and OT?
ANSWER: KOREM does not have OT assets. However, it is possible that some OT systems may be included to analyze data related to electricity generation and consumption.

QUESTION: Digital Energy Platform: Does the KOREM Digital energy platform in on prem or cloud?
ANSWER: For fault tolerance, the trading platform is still hosted in a local provider's cloud, primarily in the office server room.

QUESTION: Resource Allocation and Access: What level of access will the consulting team have to KOREM's systems and personnel?
ANSWER: The consultant will have full access to KOREM's systems and personnel. A KOREM project manager has been assigned to assist with implementation.

QUESTION: Resource Allocation and Access: How will resources be allocated for the project within KOREM? i.e., will KOREM facilitate a testing environment or grant access to the Digital Energy Platform for our team to conduct the assessment effectively.
ANSWER: KOREM will provide all necessary access and an appropriate testing environment.

QUESTION: Stakeholder Engagement: Who are the key stakeholders within KOREM and other relevant entities that need to be engaged in the project?
ANSWER: The key stakeholders shall be the Kazakhstan Electricity and Power Market Operator (KOREM) and the Kazakhstan Electricity Grid Operating Company (KEGOC).

QUESTION: Training and Capacity Building: What are the expectations for training and capacity building for KOREM's staff as part of the project?
ANSWER: Training agendas shall be developed in consultation with USEA and KOREM. The duration of the training shall not exceed the time specified in the RFP.

QUESTION: Training and Capacity Building: Are there any specific training modules or skills development that KOREM is looking to incorporate?

ANSWER: We expect the consultant to develop training agendas (in consultation with USEA and KOREM) and to suggest training modules most appropriate for the training topics specified in the RFP.

QUESTION: Training and Capacity Building: Are secure communication protocols like HTTPS and SFTP used?

ANSWER: Yes.

QUESTION: Domain in-scope for C2M2 tool: List of domains in-scope for the maturity assessment.

ANSWER: The list will be provided to the consultant once a consulting contract has been signed.