This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/010378-2023

Planning

Managed Cyber Security Operations Centre and Security Information & Event Management

National Grid Electricity System Operator LIMITED

F04: Periodic indicative notice – utilities
Periodic indicative notice only
Notice identifier: 2023/S 000-010378
Procurement identifier (OCID): ocds-h6vhtk-03bdd0
Published 11 April 2023, 3:28pm

Section I: Contracting entity

I.1) Name and addresses

National Grid Electricity System Operator LIMITED

Grand Buildings,1-3 Strand

LONDON

WC2N5EH

Contact

Christina Oates

Email

box.GP.UKBuyer@nationalgrid.com

Telephone

+44 7976989186

Country

United Kingdom

Region code

UK - United Kingdom

Companies House

11014226

Internet address(es)

Main address

https://www.nationalgrideso.com/

I.3) Communication

Additional information can be obtained from the above-mentioned address

I.6) Main activity

Electricity

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Managed Cyber Security Operations Centre and Security Information & Event Management

II.1.2) Main CPV code

- 72000000 - IT services: consulting, software development, Internet and support

II.1.3) Type of contract

Services

II.1.4) Short description

This Non-Call for Completion - RFI is the exclusive property of National Grid ESO it may not be copied, transmitted or disclosed by any means without the expressed written consent of National Grid ESO. By accepting a copy hereof, the recipient agrees to be bound by these conditions and to use these documents solely for responding to National Grid's ESO Non-Call for Competition RFI.

RFI CONTENT

This is not a formal tender process and is not being undertaken in accordance with the Utilities Contracts Regulations 2016.

Please ensure responses to all questions and any supporting documentation is clearly referenced to the question they are answering.

National Grid ESO will not be shortlisting suppliers based on their submissions and any future sourcing activities will be subject to a new event.

The RFi seeks suppliers to provide answers to the points and questions detailed in section 3 of this document.

Please provide your response to each question in a separate Word document clearly stating the question number that your response relates to. If providing any supporting information in separate documents as appropriate, state the question reference number in the file name using the following naming convention:

document name - supplier reference - question number - date

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.3) Place of performance

NUTS codes

- UK - United Kingdom

II.2.4) Description of the procurement

Your company is invited to respond to this Request for Information ("RFI") for

• the provision of an interim managed Cyber Security Operations Centre ("CSOC")

• the provision of a strategic Security Information and Events Management system ("SIEM"), and

• the provision of support to enable ESO to build and transition to an enduring in-house security operations centre.

For context, to enable the separation of the Electricity System Operator ("ESO") away from National Grid plc ("National Grid"), ESO requires a standalone cyber security capability which includes aggregation of log & event date, and 24/7 monitoring for evidence of cyber incidents.

Currently, National Grid host a group-level Security Operations Centre which monitors the estate for incidents and indicators of compromise. National Grid will continue to monitor ESO assets whilst they are being separated however, once assets are transitioned the responsibility for monitoring will transfer to ESO. ESO intend to operate an internal CSOC capability in the longer term, however, to enable the separation to proceed at-pace a partner is being sought to provide a tactical solution for 12-24 months.

Similarly, National Grid hosts its own SIEM/SOAR, (Security Orchestration, Automation and Response), solution and will continue to ingest data from ESO applications whilst they are being separated. Once environments and applications are transitioned, responsibility for ingestion of log sources will shift to ESO and therefore a solution is required to enable this. It is important for continuing operations that ESO own any vendor relationships related to SIEM and SOAR products in addition to the data contained within the products.

The purpose of this document is to provide a greater understanding of the scope of requirements, for us to understand your capabilities and your ideas, experience and recommendations in defining, selecting and delivering an integration solution-set and the partner best positioned to deliver the specified solution.

Programme Objectives

ESO is looking to select a partner to enable the successful separation of the cyber security monitoring function of the ESO away from National Grid at pace, by providing services as follows:-

• Selection and delivery of a SIEM/SOAR product or solution appropriate for the multiple complex environments ESO operate. As is it ESOs vision to transition to an internal CSOC capability in the longer-term, it is important that ESO owns any vendor relationships.

• A managed cyber security operations centre (CSOC) capability that includes 24/7 monitoring for evidence of cyber incidents, triage of events and escalation of incidents. CSOC will accommodate new environments and systems as they come online and so the solution will need to scale over time.

• Support in building an in-house CSOC, including people, process, technology, and migration planning.

To enable the separation to continue at-pace, it is required for a supplier is onboarded, SIEM/SOAR procurement has taken place and an interim CSOC solution are in place by December 2023.

Current State

ESOs separation from National Grid is marked by two key dates known as Day 1 (April 2024) and Day 2 (April 2026). To support and enable the separation programme, ESO require the selected partner to be onboarded and services noted operational by December 2023.

Day 1 marks the date that the Future System Operator is under new ownership and operation under Transitional Service Agreements (TSA) for certain services. Day 2 marks the date the enduring desired operating model for an independent Future System Operator is operational, has new industry roles, and fully exited TSAs with National Grid. Achieving the services within this RFI will ready ESO for Day 2.

Under the TSAs will be the current Incident Management processes and procedures that dovetail into the ESO Incident Management processes. Any supplier selected will need to adhere to and work with these current and future procedures.

Current Challenges

ESO is a new entity and at the beginning of the set up of its cyber security management and operational teams

ESO and National Grid, via the TSAs, must work closely together to maintain security

ESO Incident Management processes and procedures for new systems and assets, within their own foundation environment, are new and must align to any 3rd party supplier engagement

Time period until CSOC and SIEM/SOAR is operational is limited, to be achieved no later than December 2023

At a high level, the partners services should provide tools and capabilities that exceed the incumbents, complementing the platforms noted, technology, people, and processes.

This notice has been edited to remove sensitive information after publication.

II.2.14) Additional information

RFI QUESTIONS

1 Please provide details of SIEM/SOAR products with which you are able to integrate and use to provide a managed CSOC capability.

In your response, please include:

• Whether ESO are able to own the vendor relationship with any products or solutions

• Whether the products or solutions require Internet or Cloud connectivity to operate

• Whether the product or solution is a preferred or recommended vendor

• Any limitations of using a particular product or solution

2 Please summarise your experience in implementing and operating a managed Cyber Security Operations Centre (CSOC).

In your response, please include:

• Your experience in operating a managed CSOC on the customers premises

• Your experience in operating a managed CSOC remotely from your own premises

• Any industry certifications, attestations, or accreditations you hold related to your CSOC operations

3 Please summarise your experience in working with Critical National Infrastructure assets or other similar environments.

In your response, please include:

• Your approach to personnel security, including whether you employ staff subject to National Security Vetting

• Whether your delivery would be from the UK or other country

• Your use of offshore resources, assets, or storage and how this affects your service delivery

Please do not include any confidential information in your response

4 Please summarise your methodology or approach when designing, implementing a managed Cyber Security Operations Centre solution.

In your response, please include:

• Your approach to designing and defining Standard Operating Procedures

• Your approach to integrating with existing Cyber Incident Management functions

• Your approach to onboarding assets

5 Please provide at least one case-study where you have implemented and operated a

managed Cyber Security Operations Centre (CSOC) for a client.

In your response, please include:

• Your role in the overall project delivery, i.e: whether you provided only the CSOC or were a wider delivery partner

• Whether the service was delivered on customer premises or as a remotely delivered solution

• Your experience in migrating the service, such as a phased transition or switch-over

6 Please provide high-level details of your pricing structure.

In your response, please include:

• If applicable, the metrics on which your pricing structure is based, i.e: per endpoint, per GB, per hour

• Any minimum contract terms

II.3) Estimated date of publication of contract notice

31 December 2023

Section IV. Procedure

IV.1) Description

IV.1.8) Information about the Government Procurement Agreement (GPA)

The procurement is covered by the Government Procurement Agreement: Yes

IV.2) Administrative information

IV.2.2) Time limit for receipt of expressions of interest

Date

28 April 2023

Local time

12:00pm

IV.2.4) Languages in which tenders or requests to participate may be submitted

English

Section VI. Complementary information

VI.3) Additional information

The submission deadline for responses to this RFI is by 12:00 BST May 5th 2023.

Submissions must be received by the submission deadline.

Submissions should be sent to the Procurement representative for this RFI, as follows:

IT Associate Category Lead: Sarah Lewis

Contact Details: sarah.lewis@nationalgrid.com

All communications and queries arising from this RFI should be conducted on email through the Procurement Representative detailed above. Please ensure all emails on this RFI include the following in the subject box:

Integration Platform Solution Set - (suppliers reference)

Any queries must be submitted no later than 12:00 BST May 3rd 2023 for this RFI.

National Grid shall not be responsible for or pay for any costs or expenses that may be incurred by the supplier in the preparation and submission of a response to this RFI.

All details of this RFI and associated documents must be treated as private and confidential and shall not be disclosed to any other party, except where this is necessary for you to prepare and submit a response. You must ensure that you have an adequate confidentiality agreement in place with any subcontractors, consultants or agents before issuing them with any information concerning the requirements of this RFI.

Details of your response to this RFI shall not be disclosed to any third party unless such disclosure is required by law or court.