This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/022522-2023

Planning

National Grid ESO - Cyber Incident Response and Digital Forensics

NATIONAL GRID ELECTRICITY SYSTEM OPERATOR LIMITED

F04: Periodic indicative notice – utilities
Periodic indicative notice only
Notice identifier: 2023/S 000-022522
Procurement identifier (OCID): ocds-h6vhtk-03ec91
Published 2 August 2023, 5:26pm

Section I: Contracting entity

I.1) Name and addresses

NATIONAL GRID ELECTRICITY SYSTEM OPERATOR LIMITED

1-3 Strand

LONDON

WC2N 5EH

Contact

Trevor Ford

Email

box.GP.UKBuyer@nationalgrid.com

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

National Grid ESO - Cyber Incident Response and Digital Forensics

Reference number

ESO_RFI_CR_DF

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

National Grid Electricity System Operator (NGESO) moves electricity around systems to keep homes and businesses supplied with the energy they need 24/7. NGESO is a separate legal entity to National Grid Plc.

NGESO has a regulatory commitment to move all IT systems and shared services away from National Grid Plc and therefore NGESO requires a partner to provide on-demand Incident Response and Digital Forensics services aligned with NGESOs own incident management processes.

Currently, National Grid Plc provide these group-level services in-house and will continue to run these services whilst NGESO and National Grid Plc's IT environments are being separated. However, once any assets are transitioned, or when new assets are productionised into the new NGESO environments, the responsibility for Incident Response and Digital Forensics will transfer to NGESO, hence requirement for a 3rd party service to protect the business and systems.

This Non-Call for Completion Request for Information Only.

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.

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

The RFI seeks for suppliers to provide answers to the points and questions detailed in the, II.2.14) Additional information, section 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:

ESO_CIR&DF_RFI_SUPPLIER NAME

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.2) Additional CPV code(s)

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

II.2.3) Place of performance

NUTS codes

- UK - United Kingdom

II.2.4) Description of the procurement

NGESO is looking to select a partner to enable the successful separation of the cyber security Incident Response and Digital Forensics services of the NGESO away from National Grid Plc at pace, by providing services as follows:-

• Planning for Incident Response

o Help identifying the effectiveness of the service and the plugging in of missing factors

• On-demand response support in the event of a cyber incident

o 24/7 service availability

• On-demand digital forensics services

o 24/7 service availability

To enable the separation to continue at-pace, it is required for a supplier to be onboarded and services operational by January 2024.

Current State

NGESOs separation from National Grid Plc is marked by two key dates known as Day 1 (mid-2024) and Day 2 (mid-2026). To support and enable the separation programme, NGESO require the selected partner to be onboarded and services noted operational by January 2024.

Day 1 marks the date that the Future System Operator (FSO) 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 Plc. Achieving the services within this RFI will ready NGESO for Day 2.

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

Current Challenges

FSO is a new entity and is at the beginning of the set-up of its Cyber Security management and operational teams.

FSO and National Grid Plc, via their Transitional Service Agreements (TSAs), must work closely together to maintain security.

FSO's Incident Response, Digital Forensic and procurement processes for their new systems and assets, within their own foundation environment are new, and any 3rd party supplier engagement must align to them.

Time period; Managed Security Services Provider suppliers to be in place no later than January 2024.

At a high level, the future suppliers services should provide tools and capabilities that exceed

the incumbents, complementing the platforms noted, technology, people, and processes.

II.2.14) Additional information

RFI Questions

1 Please provide details of your Incident Response and Digital Forensics services, focusing on integration and including planning and response services.

In your response, please include:

• The services offered as part of your Incident Response and Digital Forensics services, including any technical or administrative limitations of the services

• How your service integrates with existing incident management procedures and practices

• Any Service Level Agreements with regards to response times in the event of an incident

2 Please summarise your prior experience in implementing and operating a managed Incident Response and Digital Forensics service.

In your response, please include:

• How long you have been providing the services

• The experience of key individuals involved in the provision and delivery of the services

• How many clients you provide Incident Response and Digital Forensics services to, both in the UK and worldwide

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 provide details of any added-value services offered either as part of, or which are complementary to your Incident Response & Digital Forensics services, for example:

• On site investigations, including for non-cyber related incidents

• Production and validation of playbooks, runbooks, Standard Operating Procedures etc.

• Facilitation of incident response exercises, table-tops, walkthroughs etc.

5 Please provide at least one case-study where you have integrated with and implemented and operated a managed Incident Response and Digital Forensics service for a client.

In your response, please include:

• The nature and level of service provided, i.e. whether your service was in addition to internal incident response services or whether you provided the service in its entirety.

• The integration approach and outcome.

• The size and scale of the organisation

• Any key successes from the service, for example incidents successfully managed limiting technical or reputational damage

Please do not include any confidential information in your response. It is not required to identify any current or former clients

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: retainer fee, per incident charges, hourly charges, per device charges etc.

• Any minimum contract terms

II.3) Estimated date of publication of contract notice

3 August 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

31 August 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 31st August 2023.

Submissions must be received by the submission deadline, submissions received after the deadline will not be considered.

Interested parties are asked to submit their Expression of Interest to this RFI by COB on the 10th August 2023.

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

Category Lead

Contact Details: To: trevor.ford@nationalgrid.com

cc: marie.glassborow@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:

"ESO_RFI_CIR&DF_SUPPLIER NAME"

Any queries must be submitted no later than 12:00 BST 15th August 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.