This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/037683-2023

Tender

Design & Build: Industrial Control System (ICS) Network

Wales & West Utilities

F05: Contract notice – utilities

Notice identifier: 2023/S 000-037683
Procurement identifier (OCID): ocds-h6vhtk-042931
Published 21 December 2023, 1:38pm

Section I: Contracting entity

I.1) Name and addresses

Wales & West Utilities

Wales & West House, Spooner Close, Coedkernew

NEWPORT

NP108FZ

Contact

Rebecca Crisp

Email

rebecca.crisp@wwutilities.co.uk

Country

United Kingdom

Region code

UKL21 - Monmouthshire and Newport

Companies House

05046791

Internet address(es)

Main address

https://www.wwutilities.co.uk/

I.3) Communication

Access to the procurement documents is restricted. Further information can be obtained at

https://sourcing4wwu.bravosolution.co.uk/web/login.html

Additional information can be obtained from the above-mentioned address

Tenders or requests to participate must be submitted electronically via

https://sourcing4wwu.bravosolution.co.uk/web/login.html

I.6) Main activity

Production, transport and distribution of gas and heat

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Design & Build: Industrial Control System (ICS) Network

Reference number

WWU1303

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

Wales & West Utilities (WWU) is embarking upon a significant programme of work to re-architect its industrial control system (ICS) networks to meet recognised best-practice architectures to ensure a secure and resilient industrial network now and for the future. WWU is seeking to partner with an organisation who can work with us on this endeavour and is interested in hearing from companies with expertise in architecting secure operational technology (OT) environments in Microsoft Azure.

This is a design and build tender, and the successful supplier will work with us on all aspects and phases of this programme, from design, through to proof of concept and testing and production deployment.

You will be required to -

- Design, document and deploy new Azure networks

- Consult, advise and design OT architecture and governance processes

- Design a layered network at Purdue layers 3 and 3.5

- Align the architecture closely to SANS ICS reference architecture

- Produce high quality architectural design documentation, to include diagrams produced in a recognised diagramming language such as UML

In order to be considered for this contract, you must meet the following requirements -

• You must be NCSC CAF assured

• You must have previous experience in designing OT/ICS architectures and the Purdue reference architecture.

• You must have prior experience of designing in Microsoft Azure environments

• Companies with this experience of undertaking similar projects in the CNI sector are of particular interest.

Please note: this tender does not include a discovery phase.

WWU would like to invite expressions of interest (EOI) based on the information specified and for interested suppliers to submit their EOI to rebecca.crisp@wwutilities.co.uk via email. They will then be invited to the PQQ which will go live on 2nd January.

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.3) Place of performance

NUTS codes

- UKK - South West (England)
- UKL - Wales

II.2.4) Description of the procurement

WWU is embarking upon a significant programme of work (called the 'Galileo Programme') to re-architect its industrial control system (ICS) networks to (a) meet recognised best-practice architectures to ensure a secure and resilient industrial network now and for the future, and (b) to take advantage of cost-effective security and resilience opportunities afforded by the cloud which exceed the possibilities afforded by the current on-premise model.

The Galileo Programme is a significant, high-risk and multi-year programme of work composed of several different phases and projects. WWU is seeking to partner with an organisation that can work closely with us on all aspects and phases of this programme, seeing it through from initial proof of concept implementations through to testing and eventual production deployment.

At the core of the programme will be the design and build of a new ICS network, including an industrial demilitarized zone (DMZ), to be hosted in Microsoft Azure. The new Azure estate will host assets at Purdue layers 3 and 3.5 and will be required to communicate securely with lower and higher layers of the WWU industrial technology stack, which are hosted outside of Azure, as well as external hosts on untrusted networks.

The project will therefore include all aspects of Azure network architecture design and implementation, including deployment of SaaS, PaaS and IaaS components as required, and will also define and implement the security policy and governance standards that will apply to the network. However, the programme also encompasses aspects that go beyond the creation of the Azure environment. For example, there is a requirement to bring unmanaged and unsupported ICS devices under proper governance and control, ensuring full lifecycle management, patching and support. Alongside this, a new solution for effective identity and access management for colleagues working in the ICS space will be required. The pros and cons of secure remote access to remote facilities will need to be considered and a secure solution implemented if WWU agrees there are security benefits to be gained. Finally, existing redundant general packet radio service (GPRS) and satellite communication (SATCOM) conduits will also need to be taken into account and factored appropriately into the new architecture design.

Objectives

1. To create an architectural design that aligns closely to the SANS ICS Reference Architecture , and which will meet WWU's business requirements for the security, safety, resilience and availability of its gas supply service.

2. To implement this design in the Microsoft Azure cloud, initially as a proof-of-concept environment, and then later developing this into formal development, test and production environments.

3. To design and establish secure network links to relevant WWU assets at layers 2 and 4, including via the use of secure 'push-pull' intermediary hosts in the DMZ.

4. To design and establish secure data exchange solutions with hosts residing in untrusted partner networks

5. To utilize Active Directory or Azure Active Directory as the identity provider for the new network and to establish effective identity and access management architectures, standards and practices for industrial colleagues.

6. To ensure all NIS-scope assets at layers 3 and 3.5 are accounted for and are securely managed throughout their operational lifecycle.

7. To establish and enforce strong security policies in the industrial network and DMZ and to establish and document secure governance practices for the new network.

8. To exploit all available Azure security tooling to the fullest extent.

Requirements

(i) Partner Requirements

Potential partners wishing to tender for this project must be able to demonstrate expertise in Microsoft Azure network design and deployment and strong familiarity and experience with the entirety of the Azure security stack. Additionally, prospective partners must be able to demonstrate expertise in ICS/OT security and the Purdue reference architecture. Preference will be given to companies who can demonstrate previous similar work with CNI customers including successful implementations of ICS networks in Azure, and the integration of those networks with higher and lower layers of the Purdue stack.

(ii) Programme Requirements

1. The partner will, having regard to WWU's core requirements for security, high availability, disaster recover, scalability, resilience and cost-effectiveness, work with the WWU Cyber Resilience team and its partners as required to design, document and deploy new Azure networks to include a new ICS layer 3 network and industrial DMZ between the ICS network and the on-prem corporate network.

2. WWU envisages that the programme will logically consist of several different phases, commencing with, design and implementation of a PoC network. Thereafter, formal testing and production deployment phases will follow. The partner will be required to work flexibly and closely with WWU and its partners throughout all of these phases, adopting agile approaches where required, and recognising that it will not necessarily be possible to fully define all requirements in advance of a phase commencing.

• With respect to the new Azure environments, the partner will be required to consult, advise and design architectures and governance processes for the secure and effective use of:

o Azure regions, availability zones and availability sets

o Azure subscription and resource group architecture

o Network design to include appropriate VNet and subnet architecture o Azure dedicated hosts

o Network and application security groups

o SaaS/PaaS/IaaS and serverless execution

o Identity and Access Management, to include user provisioning, lifecycle management, Azure Active Directory/Active Directory usage and structure, multi-factor authentication, authorisation and conditional access

o Azure managed identities

o Logging, monitoring, auditing and incident response including Sentinel integration

o Azure security components including Key Vault, Azure Firewall and Azure Web Application Firewall

o Load balancing

o Infrastructure as code & versioning, ARM templates, Terraform, Blueprints

o Azure virtual desktops

o ExpressRoute for external connectivity

o Microsoft Defender for Cloud

o Other Azure capabilities as deemed appropriate by the partner and/or WWU

4. Having regard to best-practice architecture patterns for industrial control systems, the partner will be required to work with WWU to design a layered network at Purdue layers 3 and 3.5 with appropriate vertical and horizontal segregation and major and minor enforcement boundaries as required. WWU requires the architecture to align closely to the SANS ICS reference architecture, which itself is based on the Purdue model and the requirements of ISA/IEC 62443. Key areas for architectural consideration and design will include but not necessarily be limited to:

o Defensibility and resilience

o Simple recovery

o Attack surface minimization

o Utilisation of attack trees and attack modeling to inform architectural decisions o Defence in depth across all in-scope assets

o Securing internal and external boundaries

o Creation of dedicated, function-specific subnets and dedicated DMZ zones

o Effective use of network security components including routers with ACLs, next-generation firewalls, data diodes, network and host intrusion detection and prevention

o Effective use of application-layer firewalls for web-based assets

o Identity and access management

o Secure data exchange with untrusted networks such as the WWU corporate network and external partners with whom business data relating to the essential service is shared

o Secure remote access

o Patch management

o Enablement of effective incident response via logging and monitoring

5. It will be a requirement that the partner produces high-quality architectural design documentation, to include diagrams produced in a recognised diagramming language such as UML, with sufficient accompanying narrative to make the documentation accessible to and usable by IT/OT and Security teams with no prior knowledge of the project or architecture. Nothing will be deployed without documentation and therefore the production of such documentation will be a prior or at least parallel task to the creation of new networks and resources in every case without exception.

6. Initially, the partner will use the results of the discovery phase (completed by WWU internally) to produce a documented target architecture for a PoC environment. Thereafter, and with reference to the target architecture, a PoC environment will be created that establishes a segregated ICS network and DMZ in Azure, containing a representative selection of layer 3 assets, and establishing secure links to external networks at layers 4 and 2. In this regard it is worth noting that WWU is currently building a replica gas offtake in a lab environment that can be used for L2 and below connectivity and testing.

7. Following completion of the PoC, and taking into account lessons learned, the project will then formally move into testing and finally production phases. It is not possible to be specific at this point about exactly what will be required for each of these phases and WWU therefore considers it appropriate that each major phase is planned, scoped and costed separately when requirements and timelines are clearer.

II.2.5) Award criteria

Price is not the only award criterion and all criteria are stated only in the procurement documents

II.2.7) Duration of the contract, framework agreement or dynamic purchasing system

Duration in months

60

This contract is subject to renewal

Yes

Description of renewals

Up to 3 years, in 12 month increments.

II.2.10) Information about variants

Variants will be accepted: No

II.2.11) Information about options

Options: Yes

Description of options

Up to 3 years, in 12 month increments.

Section IV. Procedure

IV.1) Description

IV.1.1) Type of procedure

Negotiated procedure with prior call for competition

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

The procurement is covered by the Government Procurement Agreement: No

IV.2) Administrative information

IV.2.2) Time limit for receipt of tenders or requests to participate

Date

19 January 2024

Local time

5:00pm

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

English

Section VI. Complementary information

VI.1) Information about recurrence

This is a recurrent procurement: No

VI.4) Procedures for review

VI.4.1) Review body

Wales & West Utilites

Newport

Country

United Kingdom