This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/023779-2023

Planning

Provision of Security Operations Centre Managed Service: Prior Information Notice

Crown Prosecution Service

F01: Prior information notice
Prior information only
Notice identifier: 2023/S 000-023779
Procurement identifier (OCID): ocds-h6vhtk-03efa8
Published 14 August 2023, 4:33pm

Section I: Contracting authority

I.1) Name and addresses

Crown Prosecution Service

102 Petty France

LONDON

SW1H 9EA

Contact

Patience Arinaitwe

Email

patience.arinaitwe@cps.gov.uk

Country

United Kingdom

Region code

UKI3 - Inner London – West

Justification for not providing organisation identifier

Not on any register

Internet address(es)

Main address

https://www.cps.gov.uk

I.3) Communication

Additional information can be obtained from the above-mentioned address

I.4) Type of the contracting authority

Ministry or any other national or federal authority

I.5) Main activity

Other activity

Security Operations Centre Managed Service

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Provision of Security Operations Centre Managed Service: Prior Information Notice

II.1.2) Main CPV code

- 72250000 - System and support services

II.1.3) Type of contract

Services

II.1.4) Short description

Provision of Security Operations Centre Managed Service Requirement: Prior Information Notice.

The Crown Prosecution Service (CPS) has a security function within the Digital and Information Directorate (DID), delivering a professional approach and striving for Security Excellence in the provision of all IT services.

Whilst the Security team is internal, the CPS is seeking to procure a Security Operations Centre (SOC) service.

The Security Operations Centre is a key service for the CPS, and it is critical that any supplier delivering this service understands the nature of the business, the key role that the CPS plays within the Criminal Justice System and the need for a full 24 x 7 x 365 security service, as there are services available outside office hours.

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.2) Additional CPV code(s)

- 72250000 - System and support services

II.2.3) Place of performance

NUTS codes

- UKI - London

II.2.4) Description of the procurement

Prior Information Notice for Provision of a Security Operations Centre (SOC) Service:

The Crown Prosecution Service (CPS) has a security function within the Digital and Information Directorate (DID), delivering a professional approach and striving for Security Excellence in the provision of all IT services.

Whilst the Security team is internal, the CPS is seeking to procure a Security Operations Centre (SOC) service.

The Security Operations Centre is a key service for the CPS, and it is critical that any supplier delivering this service understands the nature of the business, the key role that

the CPS plays within the Criminal Justice System and the need for a full 24 x 7 x 365 security service, as there are services available outside office hours.

The CPS plans to (separately) procure a SIEM tool and is looking for a SOC provider to complement its cyber defensive capabilities in providing:

· Managing the CPS SIEM solution, including:

o Onboarding / removal of SIEM feeds and/or configuration of SIEM tool

o Creating customised alerts

o 24x7x365 monitoring of alerts, including analysing alerts to detect threats and configuration of security orchestration, automation and response.

· Provide cyber threat Intelligence, including:

o Threat Intel - Identify, Investigate and hunt for cyber threats to gain insight into attacker behaviour, infrastructure, motives and IOCs'.

o Vulnerability Intelligence - identify vulnerabilities that pose the most risk to their organisation, reducing downtime, and preventing attacks.

o Supply chain intelligence - monitor the CPS's supply chain

o Brand intelligence - provide analytical insights to proactively defend against new and emerging threats to your brand, products, employees, executives, and suppliers.

· Capability integration - continually improve the detection capabilities of the SIEM by learning from cyber threat intelligence and incidents.

· Incident response, including:

o Work according to agreed incident response processes, playbooks with the customer.

o Identify, analyse, contain and eradicate, recover (see below) and review incidents.

o Provide Forensic analysis / forensic evidence gathering as required (preferably NCSC certified)

· Compliance Management - help ensure that applications, security tools and processes comply with privacy regulations, namely Data Protection Act.

The SOC provider will be expected to record incidents in the CPS ITSM tool to automate

the production of incident management information. The SOC provider will also be required to assist with the trending of incidents and attend operational level meetings with the CPS and other suppliers as required.

At this stage, the CPS is seeking to engage with the supply market as part of an information-gathering exercise to understand how suppliers might approach the provision of the services outline above, particularly with regard to any developments in SIEM / SOC delivery and innovation.

Suppliers who wish to express their interest in this potential opportunity should do so via the contact details contained within the notice and present their observations on how the requirements within this Prior Information Notice could be fulfilled.

This may take any format and should cover the following areas per as minimum:

• Observations / Comments on the customer requirements, particularly the feasibility of adding forensic analysis and NCSC certified Cyber Incident Responder retainer capability to the requirements.

• how the provision of the SOC service has been modernised in recent years

• approach to ensure Service Excellence

· Recommendation for SIEM tool(s) and reasons.

II.3) Estimated date of publication of contract notice

31 January 2024

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: No