This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/046689-2025

Contract

CCTV Shared Service Control Room Upgrade

Huntingdonshire District Council

UK7: Contract details notice - Procurement Act 2023 - view information about notice types

Notice identifier: 2025/S 000-046689
Procurement identifier (OCID): ocds-h6vhtk-055b2a (view related notices)
Published 6 August 2025, 4:53pm

Scope

Reference

C/2025/624

Description

The CCTV Shared Service Control Room forms a critical part of our public safety and security infrastructure, operating as the central hub for live surveillance, incident response, evidentiary capture, and integration with law enforcement and emergency services.

As part of its lifecycle, the control room undergoes scheduled technology refreshes approximately once every decade to remain aligned with evolving security threats, software support cycles, hardware obsolescence, and operational standards.

We have reached a mandatory upgrade point driven primarily by Microsoft's transition to Windows 11, which in turn requires a concurrent upgrade of our deployed Video Management System (VMS), Veracity (iComply).

This has now been Direct awarded and contracts signed after the mandatory standstill period following the Contract Award notice.

Contract 1. CCTV shared control room upgrade award to DSSL Group Ltd

Supplier

- DSSL GROUP LIMITED

Contract value

- £230,000 excluding VAT
- £276,000 including VAT

Above the relevant threshold

Date signed

28 July 2025

Contract dates

- 2 August 2025 to 1 October 2025
- 2 months

Main procurement category

Services

CPV classifications

- 50324100 - System maintenance services

Contract locations

- UKH12 - Cambridgeshire CC

Key performance indicators

Name
On-time Delivery Rate
Downtime / Service Interruption
Compliance with Technical Standards

Other information

Applicable trade agreements

- Government Procurement Agreement (GPA)

Conflicts assessment prepared/revised

Yes

Procedure

Procedure type

Direct award

Direct award justification

Additional or repeat goods, services or works - extension or partial replacement

1.1 Security-Sensitive Infrastructure

The existing CCTV infrastructure operates within a highly secure environment that includes:

• Internet Protocol (IP) based architecture across servers, switches, and camera networks.

• End-to-end encrypted video transmission and data storage.

• Controlled integration with police, local authority, and national security platforms.

• Role-based access controls and hardened cybersecurity policies.

Any modification to this architecture introduces inherent risks to system integrity, data protection, and operational resilience. The incumbent supplier holds full knowledge of the security architecture, encryption keys, firewall rules, VLAN segregation, failover protocols, and other critical system parameters.

1.2 Continuity of Service Obligations

The CCTV Shared Service is a 24/7 operational environment. Any prolonged downtime or system instability during the upgrade process would:

• Expose public safety risks.

• Jeopardize evidential continuity for criminal investigations.

• Breach legal and statutory obligations under GDPR, DPA, and surveillance codes of practice.

The incumbent supplier is uniquely positioned to undertake the upgrade without disruption, leveraging their intimate familiarity with existing configurations, historical issues, and contingency protocols.

2. Incumbent-Specific Configuration & Compliance Requirements

2.1 Proprietary System Configuration

The Veracity (iComply) VMS has been heavily customised over its operational life cycle, incorporating:

• Custom integration with multiple third-party data feeds (ANPR, Help Points, Blue Light integration, etc.).

• Bespoke alerting, audit trails, and control room user interfaces.

• Unique failover and recovery protocols developed by the incumbent.

Attempting to replicate or reverse-engineer these configurations via a third party would require:

• Extensive reverse engineering.

• Risk of misconfiguration.

• Loss of undocumented institutional knowledge.

2.2 Warranty, Liability & Maintenance Conflicts

• The incumbent supplier holds full responsibility for system warranties, ongoing maintenance, and post-installation support.

• Introducing a third-party installer would result in split liability and non-alignment of warranty obligations.

• Should technical issues arise post-upgrade, the incumbent would be contractually and commercially entitled to decline support on non-standard installations.

2.3 Regulatory & Audit Compliance

The incumbent supplier maintains full compliance with external and statutory audits

including SSAIB certification, which validates:

• System integrity.

• Data security.

• Operational competence.

• Resilience to cyber and physical threats.

Any deviation from the incumbent's service introduces compliance risks that may trigger adverse audit findings or even operational shutdown pending rectification

3. Access to Secure Data & Controlled Environments

3.1 Access to Sensitive Information

The upgrade process requires privileged access to:

• Historical and live surveillance footage.

• Secure server environments containing criminal investigation data.

• Law enforcement integration nodes.

• Critical physical access to secured data centres and control rooms.

The incumbent supplier already holds the required security clearances, training, and vetted personnel approved for working within these highly restricted environments.

3.2 Contractor Vetting & Validation

• Engaging new contractors would trigger extensive security vetting, vetting agency approvals, police background checks, and control room familiarisation.

• This process is time-consuming, costly, and carries the risk of failed clearances, delaying the upgrade.

• The incumbent's team remains fully cleared, trained, and embedded within current security protocols.

4. Market Comparison & Financial Analysis

4.1 Market Alternatives Considered

A comparative market assessment was undertaken to evaluate alternative suppliers and solutions, including:

• Full replacement options such as Genetec and Milestone VMS platforms.

• Re-engagement with previous suppliers offering similar solutions.

4.2 Comparative Cost Analysis

• A full system replacement was priced at approximately 400% higher than the incumbent's quoted costs due to hardware, licensing, integration, and training expenses.

• A previous supplier's proposal was 200% more expensive than the incumbent's quote for equivalent scope.

• Ancillary costs such as staff retraining, operational downtime, and interface redevelopment further inflate non-incumbent solutions.

4.3 Value for Money Conclusion

The incumbent's proposal represents:

• Full backward compatibility.

• Minimal retraining requirements.

• No service downtime.

• Lowest capital and operational expenditure.

Supplier

DSSL GROUP LIMITED

- Companies House: 06993052
- Public Procurement Organisation Number: PLTX-4334-WQWT

1-3 Britannia Court

Basildon

SS13 1EU

United Kingdom

Email: jackp@dsslgroup.co.uk

Region: UKH37 - Essex Thames Gateway

Small or medium-sized enterprise (SME): Yes

Voluntary, community or social enterprise (VCSE): No

Supported employment provider: No

Public service mutual: No

Contract 1. CCTV shared control room upgrade award to DSSL Group Ltd

---

Contracting authority

Huntingdonshire District Council

- Public Procurement Organisation Number: PXCY-8219-LWDM

Pathfinder House St Mary's Street Huntingdon,

Cambridgeshire

PE29 3TN

United Kingdom

Email: procurement@huntingdonshire.gov.uk

Region: UKH12 - Cambridgeshire CC

Organisation type: Public authority - sub-central government