PROVISION OF SECURE MULTIMEDIA TRANSFER

PR 2023 004

AWARD OF CONTRACT
BETWEEN Crown Prosecution Service and

Award Form

This Award Form creates this Contract. It summarises the main features of the procurement and includes the Buyer and the Supplier's contact details.

1.	**Buyer**	Crown Prosecution Service Based at 10th Floor, 102 Petty France, London SW1H 9EA	
2.	**Supplier**	Name: Address: Registration number: SID4GOV ID:	**Egress Software Technologies Limited** **12th Floor, white collar factory, 1 Old Street Yard, London EC1Y 8AF** **6393598**
3.	**Contract**	This Contract between the Buyer and the Supplier is for the supply of Deliverables as set out within Schedule 2 (Specification) as set against the Supplier's actual service offering as set out within Schedule 4 (Tender). This opportunity is advertised in this Contract Notice in Find A Tender, reference ITT: itt_3153 - CPS Multimedia File Transfer and Storage System (FTS Contract Notice).	
4.	**Contract reference**	**PR 2023 004**	
5.	**Buyer Cause**	Any material breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of this Contract and in respect of which the Buyer is liable to the Supplier.	
6.	**Collaborative working principles**	The Collaborative Working Principles do not apply to this Contract.	
7.	**Financial Transparency Objectives**	The Financial Transparency Objectives do not apply to this Contract.	
8.	**Start Date**	30/07/2024	

9.	**Expiry Date**	29/07/2027
10.	**Extension Period**	Contract is for 3 years, plus an option to extend by 2 further periods of 12-month's each should this option be exercised. Extension Periods may be exercised where the Buyer gives the Supplier no less than 1 Month's written notice before this Contract expires. Any Extension Periods over and above the initial 3-year term are subject to business case approval by internal governance to the Buyer to confirm spend allowance to action. Therefore, the extensions are not guaranteed to take place at Contract Start Date and the Buyer is not obliged to extend the Contract beyond the initial 3 year period. Any extension to the Contract needs to be mutually agreed by the Parties in accordance with Paragraph 5 of Schedule 3 (Charges). If the Buyer's internal sign off is not obtained, then the Parties shall either attempt to resolve any issue(s) by commercial discussion or either Party may terminate this Contract at the end of the current Review Date (as defined in Paragraph 5 of Schedule 3) and the terms of the Exit Plan (including where applicable the provision of any Termination Assistance) shall apply.
11.	**Ending this Contract without a reason**	The Buyer shall be able to terminate this Contract in accordance with Clause 14.3. Provided that the amount of notice that the Buyer shall give to terminate in Clause 14.3 shall be 90 Days.
12.	**Incorporated Terms** **(together these documents form the "this Contract")**	The following documents are incorporated into this Contract and as relevant attached to this Award Form. Where Schedule numbers are missing the Parties have agreed those Schedules are not required. If there is any conflict, the following order of precedence applies: a) This Award Form b) Any Special Terms (see **Section 14 (Special Terms)** in this Award Form) c) Schedule 31 (Buyer Specific Terms) d) Core Terms e) Schedule 36 (Intellectual Property Rights) Schedule 1 (Definitions) f) Schedule 6 (Transparency Reports) g) Schedule 20 (Processing Data) h) The following Schedules (in equal order of precedence): (i) Schedule 2 (Specification) (ii) Schedule 3 (Charges) (iii) Schedule 5 (Commercially Sensitive Information)

		(iv) Schedule 7 (Staff Transfer) (v) Schedule 8 (Implementation Plan & Testing) (vi) Schedule 9 (Installation Works) – Not Applicable (vii) Schedule 10 (Service Levels) (viii) Schedule 11 (Continuous Improvement) (ix) Schedule 12 (Benchmarking) – Not Applicable (x) Schedule 13 (Contract Management) (xi) Schedule 14 (Business Continuity and Disaster Recovery) (xii) Schedule 15 – Minimum Standards of Reliability – Not Applicable (xiii) Schedule 16 (Security) (xiv) Schedule 17 (Service Recipients) – Not Applicable (xv) Schedule 18 (Supply Chain Visibility) – Not Applicable (xvi) Schedule 19 (Cyber Essentials Scheme) (xvii) Schedule 21 (Variation Form) (xviii) Schedule 22 (Insurance Requirements) (xix) Schedule 23 (Guarantee) – Not Applicable (xx) Schedule 24 (Financial Difficulties) (xxi) Schedule 25 (Rectification Plan) (xxii) Schedule 26 (Sustainability) (xxiii) Schedule 27 (Key Subcontractors) (xxiv) Schedule 28 (ICT Services) (xxv) Schedule 28A (Agile Development) – Not Applicable (xxvi) Schedule 29 (Key Supplier Staff) (xxvii) Schedule 30 (Exit Management) (xxviii) Schedule 32 (Background Checks) – Not Applicable (xxix) Schedule 33 (Scottish Law) – Not Applicable (xxx) Schedule 34 (Northern Irish Law) – Not Applicable (xxxi) Schedule 35 (Lease Terms) – Not Applicable: (xxxii) Schedule 37 (Corporate Resolution Planning Information) – Not Applicable
		(h) Schedule 4 (Tender) which includes the responses by the Supplier to the questions asked in this Schedule 4 as set out in Appendix 1 to this Award Form. (i) Security Policy (a copy of which is included in Annex 1 to this Award Form)

13.	**Special Terms**	Special Term 1 - not applicable
		Special Term 2 – IPR There are no New IPRs in relation to this Contract, nor is any development of Third Party Software or Open Source software within the scope of the Deliverables and/or Services. Supplier Licence to Buyer The Supplier grants the Buyer a non-exclusive, revocable, non-transferable, non-sub-licensable: (a) right to permit End Users to access and use the Deliverables/Services during the Contract Period; (b) licence to install 1 copy (in object code) of the Add-Ins on End User devices; and (c) if relevant to the Services, to use any Service API. APIs may not be used for testing or to create or produce new applications. The Services and APIs are for the Buyer's business purposes only except that reports and reporting Software are for the Buyer's internal business purposes only. Access and use for personal or private use, or by or for the benefit of a third-party, is not permitted. Rights in and to the Supplier Software and Services are licensed not sold. Buyer Licence to Supplier The Buyer on its behalf and on the behalf of End Users grant the Supplier, its Affiliates and Sub-contractors a fully-paid up, non-exclusive, royalty-free, sub-licensable licence to process, copy, cache, store, display and reproduce Government Data in accordance with this Contract or in delivering the Services.
		Special Term 3 - Buyer responsibilities: The Buyer is responsible for: • determining the nature of the information to be collected, transferred and shared using the Services • Buyer side configuration and ensuring that it is carried out in accordance with the Supplier's instructions. • using (and making sure its users use) the classification, access controls and other tools and functionality provided by the Services correctly and consistency in order to appropriately protect content contained within them, or shared or transferred by use of them. • at all times ensuring that it has a lawful basis for (a) using the Services to send, share, store and receive content and for the associated processing by the Supplier and its Affiliates and Sub-processors of it in accordance with the Buyer's instructions (which includes the instructions given through the use of the classification, access controls

		and other tools and functionality provided by the Services); and (b) transferring third-party email addresses to the Supplier to enable the Buyer and its End Users to use the Services.
		Special Term 4 – Audits 1. Following a written request and subject to the confidentiality obligations set out in this Contract, the Buyer has the right no more than once per Contract Year (unless required by an applicable regulator) to audit the Supplier at the Buyer's cost. 2, The Supplier will make available to the Buyer either: • its Audit Reports (being (i) reports produced by a third-party that has audited the Supplier's compliance with third-party certification standards; or (ii), where the Supplier is not permitted to disclose the full report to the Buyer, confirmation of the audit by a valid certification of compliance); or • a bridging letter; provided that the Buyer nor its auditor is a competitor of the Supplier or its Affiliates. 3 The Buyer may use the Audit Reports to evaluate and confirm the Supplier's compliance with its obligations under this Contract (including Data Protection Legislation). 4. Subject to paragraph 5, if the Buyer can reasonably show the reports are not sufficient to meet its audit obligations under applicable data protection laws and/or to confirm the Supplier's compliance with this Contract, the Buyer or its auditor (subject signing suitable confidentiality terms) may carry out, at the Buyer's cost, an inspection at the Supplier's (but not any Subprocessors) business premises subject to such audit being: • made by written request at least 30 calendar days in advance of the proposed audit date; • undertaken during the Supplier's regular business hours, in compliance with security, access and other site policies; causing minimal disruption to the Supplier's business including its processing activities and without compromising the security and confidentiality of its services; • subject to a written scope of audit which the Supplier can change if it would, for example, without limitation, impact on its breach policies or impact its accreditations; • undertaken in the presence of a representative of the Supplier's security team or other person designated by the Supplier; and

		• subject to the Buyer ensuring a copy of the audit report being provided to the Supplier which shall be treated as the Supplier's Confidential Information. 5. If the scope of the proposed audit is covered by Audit Reports completed in the last 12 months and the Supplier confirms there are no known material changes in the controls audited, the Buyer agrees to accept those Audit Reports in lieu of requesting an audit of the controls covered by those reports.
		Special Term 5 – not applicable.
14.	**Buyer's Environmental Policy**	The Supplier agrees, in providing the Deliverables and performing its obligations under the Contract, that it will comply with Schedule 26 (Sustainability).
15.	**Social Value Commitment**	The Supplier agrees, in providing the Deliverables and performing its obligations under the Contract, to deliver the Social Value outcomes in Schedule 4 (Tender) as reflected in the Supplier's response to the question asked in that Schedule and in line with the agreed service levels and Social Value Reports to be provided as set out in Schedule 26 (Sustainability)
16.	**Buyer's Security Requirements and Security and ICT Policy**	***See*** Schedule 16 (Security) Security Requirements: as set out in Schedule 16 (Security). **Security Policy:** CPS Security Policy attached in Annex 1 to this Award Form: • For the purposes of Schedule 16 (Security) the Supplier is required to comply with the general principles of the Security Policy; • For the purposes of Supplier Staff vetting, the Supplier is required to comply with the Security Policy, save that, if there is a conflict between the terms of the Security Policy and the terms of the other Schedules then the order of precedence set out in Section 12 above shall apply. **ICT Policy:** Not Used For the purposes of Schedule 16 (Security) the Supplier is not required to comply with the ICT Policy. For the purposes of Schedule 28 (ICT) Supplier is not required to comply with the ICT Policy.
17.	**Charges**	Indexation is not applicable.

		Details in Schedule 3 (Charges) – CY = contract year Contract Year 24-25: £450,900 ex VAT Contract Year 25-26: £450,900 ex VAT Contract Year 26-27: £450,900 ex VAT Total Cost Value including 2 x 12 months possible extensions to contract Contract Year 27-28: £450,900 ex VAT Contract Year 28-29: £450,900 ex VAT Note- Extension Periods to be agreed prior to the relevant Review Date (and any subsequent Review Dates) as such term is defined in Schedule 3 with prices to be agreed as described in Paragraph 5 of Schedule 3. The possibility of these extension options does not mean that they will be agreed/accepted/confirmed by the Parties to take place at the end of year 3 or in subsequent years (if an Extension Period is agreed). **Total contract value *inc extensions*** £2,254,500 excluding VAT The detailed annual charges breakdown for the provision of services during the term will include. [redacted]

		[redacted]
18.	**Estimated Year 1 Charges**	Year 1 charge £450,900 ex VAT The Supplier shall be entitled to change the Estimated Year 1 Charges payable (as set out above) if changes are made by the Buyer to the Deliverables such as changes to the number of End Users or the storage capacity required.
19.	**Reimbursable expenses**	None
20.	**Payment method**	The payment method for this Contract is bank transfer. The payment profile is annual in advance. The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. Valid invoices must show the Purchase order number, the date of the supply, the details of the services or goods supplied, the period that the payment covers and a unique invoice number. Invoices must be submitted either directly to the Buyer's Purchase to Pay system (Oracle) or by being sent electronically to the Buyers' Authorised

		Representative. Following inspection, this will be forwarded to the Software [redacted]
21.	**Service Levels**	Service Credits will accrue in accordance with Schedule 10 (Service Levels) The Service Credit Cap is as set out in Schedule 10. The Service Period is as set out in Schedule 10. A Critical Service Level Failure is as set out in Schedule 10.
22.	**Liability**	[redacted]
23.	**Cyber Essentials Certification**	Cyber Essentials Scheme Basic Certificate (or equivalent). Details in Schedule 19 (Cyber Essentials Scheme)
24.	**Progress Meetings and Progress Reports**	The Supplier's Authorised Representative shall attend Progress Meetings with the Buyer as set out in Schedule 13 ([redacted] during the implementation phase of this Contract and as set out in Schedule 13 ([redacted]) thereafter. The Supplier shall provide the Buyer with Progress Reports every month by the 5th Working Day of each month during the implementation phase.
25.	**Guarantor**	Not Applicable
26.	**Virtual Library**	Not Applicable
27.	**Supplier's Contract Manager**	[redacted]
28.	**Supplier Authorised Representative**	Depending on the requirements (see Schedule 29 (Key Supplier Staff) for more details): [redacted]

		[redacted]
29.	**Supplier Compliance Officer**	[redacted]
30.	**Supplier Data Protection Officer**	[redacted]
31.	**Supplier Marketing Contact**	[redacted]
32.	**Key Subcontractors**	**Key Subcontractors** www.egress.com/legal/subcontractors (as amended from time to time) sets out a list of the Supplier's Subcontractors who may be involved in the delivery of the Services.
33.	**Buyer Authorised Representative**	[redacted]
34.	**Buyer's Contract Manager**	[redacted]

35.	**Buyer's Procurement Manager**	[redacted]

EXECUTION OF SIGNATURES

For and on behalf of the Supplier:		**For and on behalf of the Buyer**	
Signature:	[redacted]	Signature:	[redacted]
[redacted]	[redacted]	Name:	[redacted]
Role:	[redacted]	Role:	[redacted]
Date:	June 27, 2024 | [redacted]	Date:	June 28, 2024 | [redacted]

Annex 1

CPS Security Policy

CPS SECURITY POLICY

Section 1: Minimum Requirements

1.1 The security requirements that apply to Government Departments and Service Providers are governed by the Government's core set of mandatory minimum measures to protect information, to apply across central Government of the United Kingdom. Details of the mandatory minimum measures can be found at the Cabinet office website at:

Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk)

1.2 The general requirement is that Service Providers shall be proactive in planning and implementing appropriate policies, processes and procedures to safeguard and protect the information entrusted to them, to enable them to deliver the Service and to demonstrate that they have understood the risks relating to that information and plan mitigating action, which is then put in place and monitored.

1.3 As a minimum Service Providers shall put in place specific measures to address the access of Staff and sub-contractors: their organisation's selection and training; systems access rights; the treatment of types of information; and processes for checking compliance.

1.4 The CPS is keen to appoint Service Providers that maintain a culture of individual accountability and awareness that encourages staff to be 'trusted stewards' of sensitive data with an obligation to protect it and addresses inappropriate behaviours arising from information mismanagement.

1.5 All contracts that require IT services or integration with CPS digital systems will require IT certification in the form of the Governmental approved Cyber Essentials scheme. The UK Government have decreed all inter-linked systems that handle sensitive data and/or hold standalone sensitive data must be accredited by Cyber Essentials as a minimum. The CPS have deemed Cyber Essentials Plus will be a requirement for IT contracts or critically dependent IT systems.

1.6 The Service Provider shall hold Cyber Essentials+ and ISO 27001 certification (or the equivalent certifications) to support the delivery of the Services, at contract award. This level of certification must be maintained throughout the duration of the contract. The certification must be submitted to the CPS annually.

Section 2: Security Classification

2.1 The security classification for the CPS's mail will generally be up to Official – with the caveat of 'Sensitive' added, as the CPS deals with sensitive material as part of its criminal investigation and prosecution process. The handling of this material may additionally be subject to specific legal requirements.

2.2 The Service Provider may be expected to handle mail items consisting of live case data as part of its contracted duties. Under the previous security classifications, the possible risks of this type of information were assessed as Impact Level 3 (IL3).

2.3 As a Government department, the CPS's' operations are also subject to the Official Secrets Act. The Service Provider shall ensure that all employed Staff engaged to deliver the goods and services sign a declaration pursuant of the Official Secrets Act.

Section 3: Staff Security Requirements

3.1 The CPS deals with criminal prosecutions and the Service Provider must be aware that Service Provider Personnel may be handling live case data. All the Service Provider Personnel connected with the delivery of Service under this Contract shall be vetted to a minimum of BPSS however heightened access is required then vetting to SC standard must be considered. Any additional Service Provider Personnel nominated to work on the Contract shall also be vetted in accordance with this standard or higher where appropriate and/or necessary.

3.2 The CPS shall carry out periodic spot checks to ensure that the Service Provider Personnel have been security cleared to the appropriate level.

3.3 All of the Service Provider Personnel that can access the CPS's information or systems holding the CPS's information shall undergo regular training on secure information management principles. Unless otherwise agreed with the CPS in writing, this training shall be undertaken annually.

3.4 The Service Provider shall ensure that all Sub-Contractors engaged to deliver the goods and services work for a company approved by the CPS and comply with all security requirements.

3.5 The Service Provider shall disclose any criminal convictions (both current and spent) to which their Staff have been subject (including motoring conviction) as part of their conditions of employment and will authorise the CPS if required to carry out checks of information provided. The CPS shall have a right to insist that Staff with criminal convictions (excluding minor motoring convictions) are excluded from working on this Contract.

Section 4: General Provisions

4.1 When OFFICIAL level information or higher is held and sorted on the Service Provider premises, the premises in which it is held must be secured. The Service Provider shall ensure that material received at their premises is handled securely, including arrangements for transferring material from the delivery vehicle to the nominated premises.

4.2 The Service Provider shall ensure that suitable security measures are used by them to always ensure the security and safekeeping of the CPS's material, including transit.

4.3 The Service Provider shall have procedures in place to ensure that any material which is entrusted to their safekeeping is always stored securely and not disclosed to unauthorised staff at any time. Applying the 'principle of least privilege' the Service Provider's staff shall only be allowed access to the CPS's mail as required to ensure service delivery.

4.4 The Service Provider shall operate an access control system at its premises, via methods such as key codes and dedicated access cards, to ensure that unauthorised individuals cannot access the premises. The Service Provider shall ensure that all windows can be securely locked and operate an alarm system.

4.5 The Service Provider shall operate a Staff identification process whereby each employee is assigned a unique identifier clearly illustrating designated levels of access.

4.6 The Service Provider shall ensure that all material in their possession, in connection with delivery of the Services, is retained in the United Kingdom (UK) and is not stored or processed outside of the United Kingdom.

4.7 The Service Provider shall agree any change in location of data storage, processing, and administration with the Contracting Body in advance of any proposed move. Contracting Body data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.

4.8 The Service Provider shall allow premises to be inspected by the CPS as required, subject to advance notification, to verify the suitability of security protocols.

4.9 Should any of the material relating to the CPS's' business be unaccounted for whilst in the care of the Service Provider, the Service Provider shall trace this material within forty-eight (48) hours. Loss of any material shall be treated as a serious breach of security. Any such loss should be reported within twenty-four (24) hours to the CPS's Operational Security Team.

4.10 The Service Provider shall appreciate that public sector document provenance and data sharing security may, on occasion, be of interest to various sectors of the media. Under no circumstances should any of the CPS's' information be disclosed to external sources.

4.11 The Service Provider shall provide staff and documentation at the discretion of the CPS to demonstrate that document provenance and data sharing is robustly managed and is secure.

4.12 The Service Provider shall ensure that normal security standards are maintained in the event of a business continuity issue.

4.13 If the Service Provider receives a Right of Access (ROAR) application under the Data Protection Act (DPA) and/or the Freedom of Information (FOI) Act any such application must be notified to the CPS Representative and referred to the CPS Information Access Team's inbox before any response is made. All other DPA rights requests should be referred to the Data Protection Officer's inbox.

Section 5: Information Security Protocols

5.1 If any CPS information is held and accessed within Service Provider systems, the Service Provider shall comply with at least the minimum set of security measures and standards as determined by the Government Functional Standard GovS007 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016424/GovS_007-_Security.pdf as well as any additional protections as needed as a result of their risk assessment.

5.2 Should any service provider utilise Cloud Services in the IT deliverables then they must conform the requirements in line with NCSC's 14 Cloud Principles.

The cloud security principles - NCSC.GOV.UK

5.3 Unless otherwise agreed with the CPS in writing, all Service Provider devices used to access or manage CPS information are expected to meet the set of security requirements set out in the NCSC End User Devices Security Guidance or its successor:

Device Security Guidance - NCSC.GOV.UK

5.4 Wherever possible, such information shall be held and accessed on ICT systems on secure premises. This means Service Provider shall avoid use of removable media (including laptops, portable hard drives, CDs, USB memory sticks, tablets, and media card formats) for storage or access to such data where possible.

5.5 Where it is not possible to avoid the use of removable media, Service Provider shall apply all the following conditions:

- The information transferred to the removable media shall be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information shall be held;

- user rights to transfer data to removable media shall be carefully considered and strictly limited to ensure that this is only provided where necessary for business purposes and subject to monitoring by managers, and

- The individual responsible for the removable media shall handle it – themselves or if they entrust it to others – as if it were the equivalent of a large amount of their own cash.

- The data shall be encrypted to a UK Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, or FIPS 140-2, using software that does not require a software download onto the recipient's device.

- The data contained on the media shall be securely erased as soon as it has been transferred to a secure source.

5.6 When CPS data is held on mobile, removable, or physically uncontrolled devices or portable media, such as laptops or tablets, it shall be stored and encrypted to a UK Government standard appropriate for handling data up to and including OFFICIAL-SENSITIVE, such as FIPS 140-2 or NCSC approved methods.

5.7 Where the Service Provider grants increased IT privileges or access rights to its Staff or Sub-contractors, those persons shall be granted only those permissions necessary for them to carry out their duties and be subject to appropriate monitoring. When Staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

5.8 Service Provider shall recognise the need for the Contracting Body's information to be safeguarded under the UK Data Protection regime. To that end, Service Provider shall be able to state to the CPS the physical locations in which data may be stored, processed and managed from, and to confirm that all relevant legal and regulatory frameworks authority are complied with.

5.9 Service Provider shall agree any change in location of data storage, processing, and administration with the CPS in advance of any proposed move to the extent that such move has any impact upon the Service and relates specifically to the CPS Data. CPS Data shall not be stored outside of the UK unless agreed with the CPS's Senior Security Advisor.

5.10 The CPS requires that any information up to Official Sensitive transmitted electronically shall be sent via the Criminal Justice Secure Email (CJSM) system. The CPS will sponsor and pay for Service Provider's subscription to this system. The CJSM service is an important part of the process of joining up the Criminal Justice System (CJS) in England and Wales. It allows people working in the CJS to send emails containing information up to OFFICIAL SENSITIVE in a secure way. CJSM uses a dedicated server to securely transmit emails between connected criminal justice practitioners. Once connected, users can use CJSM to send secure emails to each other and to criminal justice organisations. As the ICT infrastructure of the CPS is updated during the Contract, Service Provider may be required to transmit data via other electronic systems, such as the 'Egress' system, but this should be agreed with the CPS Senior Security Advisor.