

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

SHORT FORM CONTRACT FOR THE SUPPLY OF GOODS AND/OR SERVICES

I. Index

I.	Index	1
II.	Cover Letter.....	3
III.	Order Form	4
IV.	Short form Terms (“Conditions”).....	9
1	Definitions used in the Contract.....	9
2	Understanding the Contract.....	17
3	How the Contract works	18
4	What needs to be delivered	18
5	Pricing and payments	20
6	The Buyer's obligations to the Supplier	21
7	Record keeping and reporting	21
8	Supplier Staff	22
9	Rights and protection.....	23
10	Intellectual Property Rights (“IPRs”)	24
11	Ending the contract.....	26
12	How much you can be held responsible for	28
13	Obeying the Law	29
14	Data Protection and Security	29
15	What you must keep confidential.....	34
16	When you can share information	36
17	Insurance	36
18	Invalid parts of the contract	36
19	Other people's rights in the contract.....	36
20	Circumstances beyond your control	37
21	Relationships created by the contract	37
22	Giving up contract rights	37
23	Transferring responsibilities.....	37
24	Supply Chain	38
25	Changing the contract.....	39
26	How to communicate about the contract	39
27	Dealing with claims	39
28	Preventing fraud, bribery and corruption	40
29	Equality, diversity and human rights	40
30	Health and safety.....	41
31	Environment and sustainability	41
32	Tax	41
33	Conflict of interest	42
34	Reporting a breach of the contract	42
35	Further Assurances	42
36	Resolving disputes.....	42
37	Which law applies	43
V.	Annex 1 – Processing Personal Data	44

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

Part A	Authorised Processing Template.....	44
Part B	Joint Controller Agreement (<i>Optional</i>)	45
1	Joint Controller Status and Allocation of Responsibilities	45
2	Undertakings of both Parties	46
3	Data Protection Breach	49
4	Audit.....	50
5	Impact Assessments.....	50
6	ICO Guidance	50
7	Liabilities for Data Protection Breach	50
8	Termination.....	52
9	Sub-Processing	52
10	Data Retention	52
Part C	Independent Controllers (<i>Optional</i>)	53
1	Independent Controller Provisions	53
VI.	Annex 2 – Specification.....	56
VII.	Annex 3 – Charges.....	59
VIII.	Annex 4 – NOT USED)	60
IX.	Annex 5 – NOT USED	61
Part A	Buyer ownership with limited Supplier rights to exploit New IPR for the purposes of the current Contract	Error! Bookmark not defined.
10	Intellectual Property Rights (“IPRs”)	Error! Bookmark not defined.
Part B	Supplier ownership of New IPR with Buyer rights for the current Contract and broader public sector functions	Error! Bookmark not defined.
10	Intellectual Property Rights (“IPRs”)	Error! Bookmark not defined.

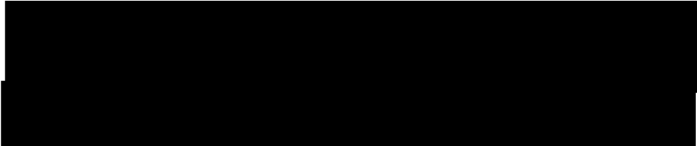
II. Cover Letter

Police Digital Services

20 Gresham Street

London

EC2V 7JE



Date: 04 November 2024

Dear Christopher Cope,

Following your proposal for the supply of cyber security assessments to The Secretary of State for the Home Department, we are pleased confirm our intention to award this Contract to you.

The attached Order Form, contract Conditions and the Annexes set out the terms of the Contract between The Secretary of State for the Home Department and Police Digital Services] for the provision of the Deliverables set out in the Order Form.

We thank you for your co-operation to date and look forward to forging a successful working relationship resulting in a smooth and successful Delivery of the Deliverables. Please confirm your acceptance of this Contract by signing and returning the Order Form to [REDACTED] at the following email address:

[REDACTED] within 7 days from the date of the Order Form. No other form of acknowledgement will be accepted. Please remember to include the reference number(s) above in any future communications relating to this Contract.

We will then arrange for the Order Form to be countersigned which will create a binding contract between us.

Yours faithfully,

[REDACTED]

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

III. Order Form

1. Contract Reference	PROJECT_18308	
2. Buyer	Secretary of State for the Home Department Home Office 2 Marsham St Peel Building London SW1 4DP In entering into this Contract, the Buyer is acting as part of the Crown and the Supplier shall be treated as contracting with the Crown as a whole.	
3. Supplier	Police Digital Service, 20 Gresham Street, London, England, EC2V 7JE, 08113293	
4. The Contract	This Contract between the Buyer and the Supplier is for the supply of Deliverables. The Supplier shall supply the Deliverables described below on the terms set out in this Order Form and the attached contract conditions (" Conditions ") and Annexes. Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions.	
5. Deliverables	Goods	NONE
	Services	in [Annex 2 – <i>Specification</i>]
6. Specification	The specification of the Deliverables is as set out in [Annex 2 – <i>Specification</i>]	
7. Start Date	01/11/2024	
8. Expiry Date	31/03/2026	

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

9. Extension Period	N/A
10. 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 the Contract and in respect of which the Buyer is liable to the Supplier.
11. Optional Intellectual Property Rights (“IPR”) Clauses	<i>Not applicable</i>
12. Charges	The Charges for the Deliverables shall be as set out • in [Annex 3 – <i>Charges</i>].
13. Payment	Payment of undisputed invoices will be made within 30 days of receipt of invoice, which must be submitted promptly by the Supplier. All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details, to: Home Office Shared Service Centre PO Box 5015 Newport NP20 9BB Within 10 Working Days of receipt of your countersigned copy of this Order Form, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, item number (if applicable) and the details (name, email, and telephone number) of your Buyer contact (i.e. Buyer Authorised Representative). Non-compliant invoices may be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment, please contact our Accounts Payable section either by email to finance-ap-enquiries@homeoffice.gov.uk or by telephone 0845 0100122

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

14. Data Protection Liability Cap	In accordance with clause 12.6 of the Conditions, the Supplier's total aggregate liability under clause 14.7.5 of the Conditions is no more than the Data Protection Liability Cap, being £500,000												
15. Progress Meetings and Progress Reports	NOT APPLICABLE												
16. Buyer Authorised Representative(s)	For general liaison your contact will continue to be 												
17. Supplier Authorised Representative(s)	For general liaison your contact will continue to be or, in their absence, 												
18. Address for notices	Secretary of State for the Home Department, Home Office 2 Marsham St, Peel Building London SW1 4DP Attention: Commercial Lead Police Digital Service, 20 Gresham Street, London, England, EC2V 7JE Attention: Head of National Audit Risk and Compliance Email:												
19. Key Staff	<table border="0" style="width: 100%;"> <thead> <tr> <th style="text-align: left;">Key Staff Role:</th> <th style="text-align: left;">Key Staff Name</th> <th style="text-align: left;">Contact Details:</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	Key Staff Role:	Key Staff Name	Contact Details:									
Key Staff Role:	Key Staff Name	Contact Details:											

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

20. Procedures and Policies	For the purposes of the Contract the: The Buyer's Staff Vetting Procedures are: The Buyer requires the Supplier to ensure that any person employed in the Delivery of the Deliverables has undertaken the disclosure and barring service or vetting checks in accordance with their employing local authority requirements. ACTSO staff have NPPV 2 (abbreviated vetting) The Buyer requires the Supplier to have undergone all due diligence in relation to the disclosure of previous appointments, and the relevant processes of the Advisory Committee on Business Appointments (ACOBA). Business appointment rules for Crown servants - GOV.UK (www.gov.uk) The Buyer's security / data security requirements are: The Buyer requires the Supplier to comply with all due diligence and good data management practise as laid out within the Contract below. Furthermore, the Buyer requires that the Supplier is undergoing the process for, or holds, SC clearance in accordance with UK Security Vetting policies for the relevant Business Area. United Kingdom Security Vetting:Referee, Supervisor, Hiring Managers and Contractors - GOV.UK (www.gov.uk).
21. Special Terms	Not Applicable
22. Incorporated Terms	The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies: - The cover letter from the Buyer to the Supplier dated 11 September 2024 (if used) - This Order Form - Any Special Terms (see row 21 (Special Terms) in this Order Form) - Terms and Conditions

The Short Form Contract

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

--	--

Signed for and on behalf of the Supplier	Signed for and on behalf of the Buyer acting on behalf of the Crown
Name: [Redacted] [Redacted]	Name: [Redacted] Commercial Lead
Date: [Redacted]	[Redacted]
[Redacted]	[Redacted]

IV. Short form Terms (“Conditions”)

1 DEFINITIONS USED IN THE CONTRACT

1.1 In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

“Affiliates”	in relation to a body corporate, any other entity which directly or indirectly Controls (in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and “ Controlled ” shall be construed accordingly), is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
“Audit”	the Buyer’s right to: (a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the Contract (including proposed or actual variations to them in accordance with the Contract); (b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Deliverables; (c) verify the Supplier’s and each Subcontractor’s compliance with the applicable Law; (d) identify or investigate actual or suspected breach of clauses 4 to 34 (inclusive), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; (e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Subcontractors or their ability to provide the Deliverables; (f) obtain such information as is necessary to fulfil the Buyer’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; (g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract; (h) carry out the Buyer’s internal and statutory audits and to prepare, examine and/or certify the Buyer’s annual and interim reports and accounts;

	(i) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Buyer has used its resources;
“Beneficiary”	A Party having (or claiming to have) the benefit of an indemnity under this Contract;
“Buyer Cause”	has the meaning given to it in the Order Form;
“Buyer”	the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;
“Charges”	the charges for the Deliverables as specified in the Order Form;
“Claim”	any claim which it appears that the Buyer is, or may become, entitled to indemnification under this Contract;
“Conditions”	means these short form terms and conditions of contract;
“Confidential Information”	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (a) is known by the receiving Party to be confidential; (b) is marked as or stated to be confidential; or (c) ought reasonably to be considered by the receiving Party to be confidential;
“Conflict of Interest”	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer;
“Contract”	the contract between the Buyer and the Supplier which is created by the Supplier’s counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes;
“Controller”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Crown Body”	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;

“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
“Data Protection Legislation”	(a) the UK GDPR, (b) the DPA 2018; (c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and (d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply);
“Data Protection Liability Cap”	has the meaning given to it in row 14 of the Order Form;
“Data Protection Officer”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Data Subject Access Request”	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
“Data Subject”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Deliver”	hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and stacking and any other specific arrangements agreed in accordance with clause 4.2. “Delivered” and “Delivery” shall be construed accordingly;
“Deliverables”	means the Goods, Services, and/or software to be supplied under the Contract as set out in the Order Form;
“DPA 2018”	the Data Protection Act 2018;
“EU GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

	personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
“Existing IPR”	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
“Expiry Date”	the date for expiry of the Contract as set out in the Order Form;
“FOIA”	the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
“Force Majeure Event”	any event, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from: (a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Party seeking to claim relief in respect of a Force Majeure Event (the “Affected Party”) which prevent or materially delay the Affected Party from performing its obligations under the Contract; (b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; (c) acts of a Crown Body, local government or regulatory bodies; (d) fire, flood or any disaster; or (e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: (a) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; (b) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and (c) any failure of delay caused by a lack of funds, and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party;
“Good Industry Practice”	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which

	would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
“Goods”	the goods to be supplied by the Supplier to the Buyer under the Contract;
“Government Data”	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Buyer's confidential information, and which: (i) are supplied to the Supplier by or on behalf of the Buyer; or (ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or (b) any Personal Data for which the Buyer is the Controller;
“Indemnifier”	a Party from whom an indemnity is sought under this Contract;
“Independent Controller”	a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data;
“Information Commissioner”	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
“Insolvency Event”	in respect of a person: (a) if that person is insolvent; (b) where that person is a company, LLP or a partnership, if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction); (c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person's assets or business; (d) if the person makes any composition with its creditors; or (e) takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction;
“IP Completion Day”	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
“Joint Controller Agreement”	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Part B Joint Controller Agreement (<i>Optional</i>) of Annex 1 – Processing Personal Data;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

“Joint Controllers”	Where two or more Controllers jointly determine the purposes and means of processing;
“Key Staff”	any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier;
“Law”	any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
“Material Breach”	a single serious breach or a number of breaches or repeated breaches (whether of the same or different obligations and regardless of whether such breaches are remedied)
“National Insurance”	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
“New IPR Items”	means a deliverable, document, product or other item within which New IPR subsists;
“New IPR”	all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR;
“Open Licence”	means any material that is published for use, with rights to access and modify, by any person for free, under a generally recognised open licence including Open Government Licence as set out at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ as updated from time to time and the Open Standards Principles documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles as updated from time to time;
“Order Form”	the order form signed by the Buyer and the Supplier printed above these Conditions;
“Party”	the Supplier or the Buyer (as appropriate) and “Parties” shall mean both of them;

“Personal Data Breach”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires and includes any breach of Data Protection Legislation relevant to Personal Data processed pursuant to the Contract;
“Personal Data”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Prescribed Person”	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in ‘Whistleblowing: list of prescribed people and bodies’, 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies as updated from time to time;
“Processor Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under the Contract;
“Processor”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Protective Measures”	technical and organisational measures which must take account of: (a) the nature of the data to be protected; (b) harm that might result from Data Loss Event; (c) state of technological development; (d) the cost of implementing any measures; including pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;
“Purchase Order Number” or “PO Number”	the Buyer’s unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the Contract;
“Rectification Plan”	the Supplier’s plan (or revised plan) to rectify its Material Breach which shall include: (a) full details of the Material Breach that has occurred, including a root cause analysis; (b) the actual or anticipated effect of the Material Breach; and

	(c) the steps which the Supplier proposes to take to rectify the Material Breach (if applicable) and to prevent such Material Breach from recurring, including timescales for such steps and for the rectification of the Material Breach (where applicable);
“Regulations”	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
“Request For Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Services”	the services to be supplied by the Supplier to the Buyer under the Contract;
“Specification”	the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;
“Staff Vetting Procedures”	vetting procedures that accord with Good Industry Practice or, where applicable, the Buyer’s procedures or policies for the vetting of personnel as specified in the Order Form or provided to the Supplier in writing following agreement to the same by the Supplier from time to time;
“Start Date”	the start date of the Contract set out in the Order Form;
“Sub-Contract”	any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: (a) provides the Deliverables (or any part of them); (b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or (c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
“Subcontractor”	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
“Subprocessor”	any third party appointed to process Personal Data on behalf of the Processor related to the Contract;
“Supplier Staff”	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Contract;
“Supplier”	the person named as Supplier in the Order Form;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

“Term”	the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract;
“Third Party IPR”	intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
“Transparency Information”	In relation to Contracts with a value above the relevant threshold set out in Part 2 of the Regulations only, the content of the Contract, including any changes to this Contract agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Contract required to be published by the Buyer to comply with its transparency obligations, including those set out in Public Procurement Policy Note 09/21 (update to legal and policy requirements to publish procurement information on Contracts Finder) (https://www.gov.uk/government/publications/ppn-0921-requirements-to-publish-on-contracts-finder) as updated from time to time and Public Procurement Policy Note 01/17 (update to transparency principles) where applicable (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles) as updated from time to time except for: (a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and (b) Confidential Information;
“UK GDPR”	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4);
“VAT”	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
“Worker”	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) as updated from time to time applies in respect of the Deliverables; and
“Working Day”	a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

2 UNDERSTANDING THE CONTRACT

2.1 In the Contract, unless the context otherwise requires:

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 2.1.1 references to numbered clauses are references to the relevant clause in these Conditions;
- 2.1.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 2.1.3 references to “writing” include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;
- 2.1.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated, replaced or re-enacted from time to time (including as a consequence of the Retained EU Law (Revocation and Reform) Act) and to any legislation or byelaw made under that Law;
- 2.1.5 the word “including”, “for example” and similar words shall be understood as if they were immediately followed by the words “without limitation”;
- 2.1.6 any reference which, immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to section 1A of the European Union (Withdrawal) Act 2018), is a reference to (as it has effect from time to time) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (“**EU References**”) which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 and which shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time.

3 HOW THE CONTRACT WORKS

- 3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.
- 3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.
- 3.3 The Supplier warrants and represents that its tender (if any) and all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

4 WHAT NEEDS TO BE DELIVERED

4.1 All Deliverables

- 4.1.1 The Supplier must provide Deliverables:
 - 4.1.1.1 in accordance with the Specification, the tender (where applicable) and the Contract;
 - 4.1.1.2 using reasonable skill and care;
 - 4.1.1.3 using Good Industry Practice;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

4.1.1.4 using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract;

4.1.1.5 on the dates agreed; and

4.1.1.6 that comply with all Law.

4.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

4.2 Goods clauses

4.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

4.2.2 The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.

4.2.3 Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

4.2.4 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

4.2.5 The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).

4.2.6 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

4.2.7 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

4.2.8 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

4.2.9 The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.

4.2.10 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.

4.2.11 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 4.2.12 The Buyer will not be liable for any actions, claims, costs and expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.

4.3 Services clauses

- 4.3.1 Late Delivery of the Services will be a default of the Contract.
- 4.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the security requirements (where any such requirements have been provided).
- 4.3.3 The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services.
- 4.3.4 The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.
- 4.3.5 The Supplier must allocate sufficient resources and appropriate expertise to the Contract.
- 4.3.6 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- 4.3.7 On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.
- 4.3.8 The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality and free from defects.
- 4.3.9 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

5 PRICING AND PAYMENTS

- 5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.
- 5.2 All Charges:
- 5.2.1 exclude VAT, which is payable on provision of a valid VAT invoice; and

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

5.2.2 include all costs and expenses connected with the supply of Deliverables.

5.3 The Buyer must pay the Supplier the charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the invoice or in the Order Form.

5.4 A Supplier invoice is only valid if it:

5.4.1 includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer; and

5.4.2 includes a detailed breakdown of Deliverables which have been delivered.

5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 36.

5.6 The Buyer may retain, or set-off payment of any amount owed to it by the Supplier under this Contract or any other agreement between the Supplier and the Buyer if notice and reasons are provided.

5.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, the Buyer can publish the details of the late payment or non-payment.

6 THE BUYER'S OBLIGATIONS TO THE SUPPLIER

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

6.1.1 the Buyer cannot terminate the Contract under clause 11;

6.1.2 the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;

6.1.3 the Supplier is entitled to additional time needed to deliver the Deliverables; and

6.1.4 the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:

6.2.1 gives notice to the Buyer within 10 Working Days of becoming aware;

6.2.2 demonstrates that the failure only happened because of the Buyer Cause; and

6.2.3 mitigated the impact of the Buyer Cause.

7 RECORD KEEPING AND REPORTING

7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the date of expiry or termination of the Contract and in accordance with the UK GDPR or the EU GDPR as the context requires.
- 7.3 The Supplier must allow any auditor appointed by the Buyer access to its premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the Audit.
- 7.4 The Buyer or an auditor can Audit the Supplier.
- 7.5 During an Audit, the Supplier must provide information to the auditor and reasonable co-operation at their request.
- 7.6 The Parties will bear their own costs when an Audit is undertaken unless the Audit identifies a Material Breach by the Supplier, in which case the Supplier will repay the Buyer's reasonable costs in connection with the Audit.
- 7.7 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:
- 7.7.1 tell the Buyer and give reasons;
 - 7.7.2 propose corrective action; and
 - 7.7.3 provide a deadline for completing the corrective action.
- 7.8 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:
- 7.8.1 require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and
 - 7.8.2 if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for Material Breach (or on such date as the Buyer notifies) and the consequences of termination in Clause 11.5.1 shall apply.
- 7.9 If there is a Material Breach, the Supplier must notify the Buyer within 3 Working Days of the Supplier becoming aware of the Material Breach. The Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional documentation that the Buyer requires. Once such Rectification Plan is agreed between the Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.

8 SUPPLIER STAFF

- 8.1 The Supplier Staff involved in the performance of the Contract must:

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 8.1.1 be appropriately trained and qualified;
 - 8.1.2 be vetted in accordance with the Staff Vetting Procedures; and
 - 8.1.3 comply with all conduct requirements when on the Buyer's premises.
- 8.2 Where the Buyer decides one of the Supplier's Staff isn't suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.
- 8.3 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.
- 8.4 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.
- 8.5 The Buyer indemnifies the Supplier against all claims brought by any person employed or engaged by the Buyer caused by an act or omission of the Buyer or any of the Buyer's employees, agents, consultants and contractors.
- 8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:
 - 8.6.1 requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 8.6.2 the person concerned resigns, retires or dies or is on parental or long-term sick leave; or
 - 8.6.3 the person's employment or contractual arrangement with the Supplier or any Subcontractor is terminated for material breach of contract by the employee.
- 8.7 The Supplier shall ensure that no person who discloses that they have a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a disclosure and barring service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

9 RIGHTS AND PROTECTION

- 9.1 The Supplier warrants and represents that:
 - 9.1.1 it has full capacity and authority to enter into and to perform the Contract;
 - 9.1.2 the Contract is entered into by its authorised representative;
 - 9.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;
 - 9.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 9.1.5 all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;
- 9.1.6 it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and
- 9.1.7 it is not impacted by an Insolvency Event.

9.2 The warranties and representations in clause 3.3 and clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.

9.3 The Supplier indemnifies the Buyer against each of the following:

- 9.3.1 wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and
- 9.3.2 non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty made in relation to the Contract that becomes untrue or misleading, it must immediately notify the Buyer.

9.5 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier for free.

10 INTELLECTUAL PROPERTY RIGHTS ("IPRS")

10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable worldwide licence to use, copy and adapt the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:

- 10.1.1 receive and use the Deliverables; and
- 10.1.2 use the New IPR.

The termination or expiry of the Contract does not terminate any licence granted under this clause 10.

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

10.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 10.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract, it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.
- 10.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 10 or otherwise agreed in writing.
- 10.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an **"IPR Claim"**), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.
- 10.7 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:
- 10.7.1 obtain for the Buyer the rights in clause 10.1 without infringing any third party intellectual property rights; and
 - 10.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.
 - 10.7.3 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clauses 11.5.1 shall apply.
- 10.8 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:
- 10.8.1 the Buyer gives its approval to do so; and
 - 10.8.2 one of the following conditions applies:
 - 10.8.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 10.1; or
 - 10.8.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 10.8.2.1:
 - (a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;
 - (b) the Buyer agrees to those licence terms; and
 - (c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or
 - 10.8.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 10.9 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

11 ENDING THE CONTRACT

- 11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.
- 11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.

11.3 Ending the Contract without a reason

- 11.3.1 The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice, and if it's terminated clause 11.6.2 applies.

11.4 When the Buyer can end the Contract

- 11.4.1 If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier and the consequences of termination in Clause 11.5.1 shall apply:
- 11.4.1.1 there's a Supplier Insolvency Event;
 - 11.4.1.2 the Supplier is in Material Breach of the Contract;
 - 11.4.1.3 there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;
 - 11.4.1.4 the Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded;
 - 11.4.1.5 the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them; or
 - 11.4.1.6 the Supplier fails to comply with its legal obligations in the fields of environmental, social, equality or employment Law when providing the Deliverables.
- 11.4.2 If any of the events in 73(1) (a) or (b) of the Regulations happen, the Buyer has the right to immediately terminate the Contract and clauses 11.5.1.2 to 11.5.1.7 apply.

11.5 What happens if the Contract ends

- 11.5.1 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data (if used), all of the following apply:

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 11.5.1.1 the Supplier is responsible for the Buyer's reasonable costs of procuring replacement Deliverables for the rest of the term of the Contract;
- 11.5.1.2 the Buyer's payment obligations under the terminated Contract stop immediately;
- 11.5.1.3 accumulated rights of the Parties are not affected;
- 11.5.1.4 the Supplier must promptly delete or return the Government Data except where required to retain copies by Law;
- 11.5.1.5 the Supplier must promptly return any of the Buyer's property provided under the Contract;
- 11.5.1.6 the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement; and
- 11.5.1.7 the Supplier must repay to the Buyer all the Charges that it has been paid in advance for Deliverables that it has not provided as at the date of termination or expiry.

11.5.2 The following clauses survive the expiry or termination of the Contract: 1, 4.2.9, 5, 7, 8.4, 10, 11.5, 12, 14, 15, 16, 18, 19, 32.2.2, 36 and 37 and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination)

- 11.6.1 The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.
- 11.6.2 Where the Buyer terminates the Contract in accordance with clause 11.3 or the Supplier terminates the Contract under clause 11.6 or 23.4:
 - 11.6.2.1 the Buyer must promptly pay all outstanding charges incurred by the Supplier;
 - 11.6.2.2 the Buyer must pay the Supplier reasonable committed and unavoidable losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated; and
 - 11.6.2.3 clauses 11.5.1.2 to 11.5.1.7 apply.
- 11.6.3 The Supplier also has the right to terminate the Contract in accordance with Clauses 20.3 and 23.4.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

11.7 Partially ending and suspending the Contract

- 11.7.1 Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.
- 11.7.2 The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.
- 11.7.3 The Parties must agree (in accordance with clause 25) any necessary variation required by clause 11.7, but the Supplier may not either:
 - 11.7.3.1 reject the variation; or
 - 11.7.3.2 increase the Charges, except where the right to partial termination is under clause 11.3.
- 11.7.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12 HOW MUCH YOU CAN BE HELD RESPONSIBLE FOR

- 12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than 125% of the Charges paid or payable to the Supplier.
- 12.2 No Party is liable to the other for:
 - 12.2.1 any indirect losses; and/or
 - 12.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).
- 12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:
 - 12.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
 - 12.3.2 its liability for bribery or fraud or fraudulent misrepresentation by it or its employees; or
 - 12.3.3 any liability that cannot be excluded or limited by Law.
- 12.4 In spite of clause 12.1, the Supplier does not limit or exclude its liability for any indemnity given under clauses 8.4, 9.3.2, 10.6, or 32.2.2.
- 12.5 In spite of clause 12.1, the Buyer does not limit or exclude its liability for any indemnity given under clause 8.5.
- 12.6 Notwithstanding clause 12.1, but subject to clauses 12.1 and 12.3, the Supplier's total aggregate liability under clause 14.7.5 shall not exceed the Data Protection Liability Cap.
- 12.7 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.
- 12.8 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13 OBEYING THE LAW

13.1 The Supplier, in connection with provision of the Deliverables:

- 13.1.1 is expected to meet and have its Subcontractors meet the standards set out in the Supplier Code of Conduct:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdf) as such Code of Conduct may be updated from time to time, and such other sustainability requirements as set out in the Order Form. The Buyer also expects to meet this Code of Conduct;
- 13.1.2 must comply with the provisions of the Official Secrets Acts 1911 to 1989 and section 182 of the Finance Act 1989;
- 13.1.3 must support the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010;
- 13.1.4 must comply with the model contract terms contained in (a) to (m) of Annex C of the guidance to [PPN 02/23 \(Tackling Modern Slavery in Government Supply Chains\)](#),¹ as such clauses may be amended or updated from time to time; and
- 13.1.5 meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: <https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>, as updated from time to time.

13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.

13.3 The Supplier must appoint a compliance officer who must be responsible for ensuring that the Supplier complies with Law, clause 13.1 and clauses 27 to 34.

14 DATA PROTECTION AND SECURITY

- 14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.
- 14.2 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies via secure encrypted method upon reasonable request.
- 14.3 The Supplier must ensure that any Supplier, Subcontractor, or Subprocessor system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified in the Order Form or otherwise in writing by the Buyer (where any such requirements have been provided).
- 14.4 If at any time the Supplier suspects or has reason to believe that the Government Data is corrupted, lost or sufficiently degraded, then the Supplier must immediately notify the Buyer and suggest remedial action.

¹ <https://www.gov.uk/government/publications/ppn-0223-tackling-modern-slavery-in-government-supply-chains>

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 14.5 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
- 14.5.1 tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
 - 14.5.2 restore the Government Data itself or using a third party.
- 14.6 The Supplier must pay each Party's reasonable costs of complying with clause 14.5 unless the Buyer is at fault.
- 14.7 The Supplier:
- 14.7.1 must provide the Buyer with all Government Data in an agreed format (provided it is secure and readable) within 10 Working Days of a written request;
 - 14.7.2 must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
 - 14.7.3 must securely destroy all storage media that has held Government Data at the end of life of that media using Good Industry Practice, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers;
 - 14.7.4 securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers; and
 - 14.7.5 indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.
- 14.8 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:
- 14.8.1 "Controller" in respect of the other Party who is "Processor";
 - 14.8.2 "Processor" in respect of the other Party who is "Controller";
 - 14.8.3 "Joint Controller" with the other Party;
 - 14.8.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",
- in respect of certain Personal Data under the Contract and shall specify in Part A Authorised Processing Template of Annex 1 – Processing Personal Data which scenario they think shall apply in each situation.

14.9 Where one Party is Controller and the other Party its Processor

- 14.9.1 Where a Party is a Processor, the only processing that the Processor is authorised to do is listed in Part A Authorised Processing Template of Annex 1 – Processing Personal Data by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).
- 14.9.2 The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.
- 14.9.3 The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, which may include, at the discretion of the Controller:
 - 14.9.3.1 a systematic description of the expected processing and its purpose;
 - 14.9.3.2 the necessity and proportionality of the processing operations;
 - 14.9.3.3 the risks to the rights and freedoms of Data Subjects; and
 - 14.9.3.4 the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.
- 14.9.4 The Processor must, in relation to any Personal Data processed under this Contract:
 - 14.9.4.1 process that Personal Data only in accordance with Part A Authorised Processing Template of Annex 1 – Processing Personal Data unless the Processor is required to do otherwise by Law. If lawful to notify the Controller, the Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.
 - 14.9.4.2 put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.
 - 14.9.4.3 Ensure that:
 - (a) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Part A Authorised Processing Template of Annex 1 – Processing Personal Data);
 - (b) it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (i) are aware of and comply with the Processor's duties under this clause 14;
 - (ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- (iii) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and
 - (iv) have undergone adequate training in the use, care, protection and handling of Personal Data.
- (c) the Processor must not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (d) the transfer is in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or
- (e) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:
 - (i) where the transfer is subject to UK GDPR:
 - (A) the International Data Transfer Agreement (the “**IDTA**”), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018 as well as any additional measures determined by the Controller;
 - (B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (“**EU SCCs**”), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the “**Addendum**”) as published by the Information Commissioner's Office from time to time; and/or
 - (ii) where the transfer is subject to EU GDPR, the EU SCCs, as well as any additional measures determined by the Controller being implemented by the importing party;
- (f) the Data Subject has enforceable rights and effective legal remedies when transferred;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- (g) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
 - (h) the Processor complies with the Controller's reasonable prior instructions about the processing of the Personal Data.
- 14.9.5 The Processor must at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 14.9.6 The Processor must notify the Controller immediately if it:
 - 14.9.6.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 14.9.6.2 receives a request to rectify, block or erase any Personal Data;
 - 14.9.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 14.9.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
 - 14.9.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and
 - 14.9.6.6 becomes aware of a Data Loss Event.
- 14.9.7 Any requirement to notify under clause 14.9.6 includes the provision of further information to the Controller in stages as details become available.
- 14.9.8 The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.9.6. This includes giving the Controller:
 - 14.9.8.1 full details and copies of the complaint, communication or request;
 - 14.9.8.2 reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
 - 14.9.8.3 any Personal Data it holds in relation to a Data Subject on request;
 - 14.9.8.4 assistance that it requests following any Data Loss Event; and
 - 14.9.8.5 assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

14.9.9 The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:

14.9.9.1 is not occasional;

14.9.9.2 includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

14.9.9.3 is likely to result in a risk to the rights and freedoms of Data Subjects.

14.9.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

14.9.11 Before allowing any Subprocessor to process any Personal Data, the Processor must:

14.9.11.1 notify the Controller in writing of the intended Subprocessor and processing;

14.9.11.2 obtain the written consent of the Controller;

14.9.11.3 enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor; and

14.9.11.4 provide the Controller with any information about the Subprocessor that the Controller reasonably requires.

14.9.12 The Processor remains fully liable for all acts or omissions of any Subprocessor.

14.9.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority.

14.10 Joint Controllers of Personal Data

14.10.1 In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data.

14.11 Independent Controllers of Personal Data

14.11.1 In the event that the Parties are Independent Controllers in respect of Personal Data under the Contract, the terms set out in Part C Independent Controllers (*Optional*) of Annex 1 – Processing Personal Data shall apply to this Contract.

15 WHAT YOU MUST KEEP CONFIDENTIAL

15.1 Each Party must:

15.1.1 keep all Confidential Information it receives confidential and secure;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 15.1.2 not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and
 - 15.1.3 immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.
- 15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:
 - 15.2.1 where disclosure is required by applicable Law if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
 - 15.2.2 if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;
 - 15.2.3 if the information was given to it by a third party without obligation of confidentiality;
 - 15.2.4 if the information was in the public domain at the time of the disclosure;
 - 15.2.5 if the information was independently developed without access to the disclosing Party's Confidential Information;
 - 15.2.6 on a confidential basis, to its auditors or for the purposes of regulatory requirements;
 - 15.2.7 on a confidential basis, to its professional advisers on a need-to-know basis; and
 - 15.2.8 to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.
- 15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.
- 15.4 The Buyer may disclose Confidential Information in any of the following cases:
 - 15.4.1 on a confidential basis to the employees, agents, consultants and contractors of the Buyer;
 - 15.4.2 on a confidential basis to any Crown Body, any successor body to a Crown Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;
 - 15.4.3 if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
 - 15.4.4 where requested by Parliament; and
 - 15.4.5 under clauses 5.7 and 16.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.
- 15.6 Transparency Information, and Information which is exempt from disclosure by clause 16 is not Confidential Information.
- 15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16 WHEN YOU CAN SHARE INFORMATION

- 16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.
- 16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, the Supplier must give the Buyer full co-operation and information needed so the Buyer can:
- 16.2.1 comply with any Request For Information
 - 16.2.2 if the Contract has a value over the relevant threshold in Part 2 of the Regulations, comply with any of its obligations in relation to publishing Transparency Information.
- 16.3 To the extent that it is allowed and practical to do so, the Buyer will use reasonable endeavours to notify the Supplier of a Request For Information and may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer's decision in its absolute discretion.

17 INSURANCE

- 17.1 The Supplier shall ensure it has adequate insurance cover for this Contract.

18 INVALID PARTS OF THE CONTRACT

- 18.1 If any provision or part-provision of this Contract is or becomes invalid, illegal or unenforceable for any reason, such provision or part-provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Contract. The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements, or agreements whether written or oral. No other provisions apply.

19 OTHER PEOPLE'S RIGHTS IN THE CONTRACT

- 19.1 No third parties may use the Contracts (Rights of Third Parties) Act ("CRTPA") to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

20 CIRCUMSTANCES BEYOND YOUR CONTROL

- 20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:
- 20.1.1 provides written notice to the other Party; and
 - 20.1.2 uses all reasonable measures practical to reduce the impact of the Force Majeure Event.
- 20.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.
- 20.3 Either Party can partially or fully terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously and the consequences of termination in Clauses 11.5.1.2 to 11.5.1.7 shall apply.
- 20.4 Where a Party terminates under clause 20.3:
- 20.4.1 each Party must cover its own losses; and
 - 20.4.2 clauses 11.5.1.2 to 11.5.1.7 apply.

21 RELATIONSHIPS CREATED BY THE CONTRACT

- 21.1 The Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22 GIVING UP CONTRACT RIGHTS

- 22.1 A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

23 TRANSFERRING RESPONSIBILITIES

- 23.1 The Supplier cannot assign, novate or in any other way dispose of the Contract or any part of it without the Buyer's written consent.
- 23.2 The Buyer can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.
- 23.3 When the Buyer uses its rights under clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.
- 23.4 The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.
- 23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

24 SUPPLY CHAIN

- 24.1 The Supplier cannot sub-contract the Contract or any part of it without the Buyer's prior written consent. The Supplier shall provide the Buyer with the name of any Subcontractor the Supplier proposes to engage for the purposes of the Contract. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. If the Buyer does not communicate a decision to the Supplier within 10 Working Days of the request for consent then its consent will be deemed to have been given. The Buyer may reasonably withhold its consent to the appointment of a Subcontractor if it considers that:
- 24.1.1 the appointment of a proposed Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 24.1.2 the proposed Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 24.1.3 the proposed Subcontractor employs unfit persons.
- 24.2 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:
- 24.2.1 their name;
 - 24.2.2 the scope of their appointment; and
 - 24.2.3 the duration of their appointment.
- 24.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.
- 24.4 For Sub-Contracts in the Supplier's supply chain entered into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract:
- 24.4.1 where such Sub-Contracts are entered into after the Start Date, the Supplier will ensure that they all contain provisions that; or
 - 24.4.2 where such Sub-Contracts are entered into before the Start Date, the Supplier will take all reasonable endeavours to ensure that they all contain provisions that:
 - 24.4.2.1 allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law;
 - 24.4.2.2 require the Supplier to pay all Subcontractors in full, within 30 days of receiving a valid, undisputed invoice; and
 - 24.4.2.3 allow the Buyer to publish the details of the late payment or non-payment if this 30-day limit is exceeded.
- 24.5 At the Buyer's request, the Supplier must terminate any Sub-Contracts in any of the following events:
- 24.5.1 there is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 of a Subcontractor which isn't pre-approved by the Buyer in writing;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 24.5.2 the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 11.4;
- 24.5.3 a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer;
- 24.5.4 the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law; and/or
- 24.5.5 the Buyer has found grounds to exclude the Subcontractor in accordance with Regulation 57 of the Regulations.

24.6 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.

25 CHANGING THE CONTRACT

25.1 Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.

26 HOW TO COMMUNICATE ABOUT THE CONTRACT

- 26.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9am on the first Working Day after sending unless an error message is received.
- 26.2 Notices to the Buyer or Supplier must be sent to their address or email address in the Order Form.
- 26.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

27 DEALING WITH CLAIMS

- 27.1 If a Beneficiary becomes aware of any Claim, then it must notify the Indemnifier as soon as reasonably practical.
- 27.2 at the Indemnifier's cost the Beneficiary must:
 - 27.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim;
 - 27.2.2 give the Indemnifier reasonable assistance with the Claim if requested; and
 - 27.2.3 not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.
- 27.3 The Beneficiary must:
 - 27.3.1 consider and defend the Claim diligently and in a way that does not damage the Beneficiary's reputation; and

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 27.3.2 not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

28 PREVENTING FRAUD, BRIBERY AND CORRUPTION

28.1 The Supplier shall not:

- 28.1.1 commit any criminal offence referred to in 57(1) and 57(2) of the Regulations; or
- 28.1.2 offer, give, or agree to give anything, to any person (whether working for or engaged by the Buyer or any other public body) an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other public function or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any other public function.

28.2 The Supplier shall take all reasonable endeavours (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with Good Industry Practice, to prevent any matters referred to in clause 28.1 and any fraud by the Supplier Staff and the Supplier (including its shareholders, members and directors) in connection with the Contract and shall notify the Buyer immediately if it has reason to suspect that any such matters have occurred or is occurring or is likely to occur.

28.3 If the Supplier notifies the Buyer as required by clause 28.2, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

28.4 If the Supplier or the Supplier Staff engages in conduct prohibited by clause 28.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:

- 28.4.1 require the Supplier to remove any Supplier Staff from providing the Deliverables if their acts or omissions have caused the default; and
- 28.4.2 immediately terminate the Contract and the consequences of termination in Clause 11.5.1 shall apply.

29 EQUALITY, DIVERSITY AND HUMAN RIGHTS

29.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:

- 29.1.1 protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
- 29.1.2 any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 29.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

30 HEALTH AND SAFETY

- 30.1 The Supplier must perform its obligations meeting the requirements of:
- 30.1.1 all applicable Law regarding health and safety; and
 - 30.1.2 the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.
- 30.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

31 ENVIRONMENT AND SUSTAINABILITY

- 31.1 In performing its obligations under the Contract, the Supplier shall, to the reasonable satisfaction of the Buyer:
- 31.1.1 meet, in all material respects, the requirements of all applicable Laws regarding the environment; and
 - 31.1.2 comply with its obligations under the Buyer's current environmental policy, which the Buyer must provide, and make Supplier Staff aware of such policy.

32 TAX

- 32.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.
- 32.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Contract, the Supplier must both:
- 32.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
 - 32.2.2 indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.
- 32.3 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains requirements that:

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 32.3.1 the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 32.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
- 32.3.2 the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
- 32.3.3 the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with clause 32.2 or confirms that the Worker is not complying with those requirements; and
- 32.3.4 the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

33 CONFLICT OF INTEREST

- 33.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual, potential or perceived Conflict of Interest.
- 33.2 The Supplier must promptly notify and provide details to the Buyer if an actual, potential or perceived Conflict of Interest happens or is expected to happen.
- 33.3 The Buyer will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Buyer, such measures do not or will not resolve an actual or potential conflict of interest, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and Clauses 11.5.1.2 to 11.5.1.7 shall apply.

34 REPORTING A BREACH OF THE CONTRACT

- 34.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13.1, or clauses 27 to 33.
- 34.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 34.1 to the Buyer or a Prescribed Person.

35 FURTHER ASSURANCES

- 35.1 Each Party will, at the request and cost of the other Party, do all things which may be reasonably necessary to give effect to the meaning of this Contract.

36 RESOLVING DISPUTES

- 36.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 36.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (“**CEDR**”) Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 36.3 to 36.5.
- 36.3 Unless the Buyer refers the dispute to arbitration using clause 36.4, the Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction. :
- 36.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.
- 36.5 The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 36.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 36.4.
- 36.6 The Supplier cannot suspend the performance of the Contract during any dispute.

37 WHICH LAW APPLIES

- 37.1 This Contract and any issues or disputes arising out of, or connected to it, are governed by English law.

V. Annex 1 – Processing Personal Data**Part A Authorised Processing Template**

This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

The contact details of the Controller's Data Protection Officer are: dpo@homeoffice.gov.uk

The contact details of the Processor's Data Protection Officer are: **[Insert Contact details]**

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Annex.

Description of authorised processing	Details
Identity of Controller and Processor / Independent Controllers / Joint Controllers for each category of Personal Data	<i>This is a call of contract in which external organisations are applying for access to Home Office built systems. The personal data on those systems is controlled by NPCC. However, the personal data is not being processed through this contract.</i>
Subject matter of the processing	There is no personal data processing.
Duration of the processing	4-6 weeks activity per call off contract. However there is no personal data processing.
Nature and purposes of the processing	There is no personal data processing.
Type of Personal Data being processed	There is no personal data processing.
Categories of Data Subject	There is no personal data processing.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	There is no personal data processing.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract and International transfers and legal gateway	There is no personal data processing.
Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect Personal Data processed under this Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event	There is no personal data processing.

Part B Joint Controller Agreement (*Optional*)

1 JOINT CONTROLLER STATUS AND ALLOCATION OF RESPONSIBILITIES

1.1 With respect to Personal Data for which the Parties are Joint Controllers, the Parties envisage that they shall each be a Controller in respect of that Personal Data in accordance with the terms of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data in replacement of Clauses 14.9 to 14.9.13 of the Conditions of this Contract. Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controllers.

1.2 The Parties agree that the **[Supplier/Buyer]**:

- 1.2.1 is the exclusive point of contact for Data Subjects and is responsible for using best endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- 1.2.2 shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- 1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- 1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for processing in connection with the Deliverables where consent is the relevant legal basis for that processing; and

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

1.2.5 shall make available to Data Subjects the essence of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Buyer's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of paragraph 1.2 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2 UNDERTAKINGS OF BOTH PARTIES

2.1 The Supplier and the Buyer each undertake that they shall:

- 2.1.1 report to the other Party every [x] months on:
 - 2.1.1.1 the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
 - 2.1.1.2 the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - 2.1.1.3 any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
 - 2.1.1.4 any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
 - 2.1.1.5 any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,
- that it has received in relation to the subject matter of the Contract during that period;
- 2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1.1 to 2.1.1.5 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data;
- 2.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 1.2 and 2.1.1.3 to 2.1.1.5 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data; to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this of this of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data;
- 2.1.5 request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- 2.1.6 ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- 2.1.7 use best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that Processor Personnel:
 - 2.1.7.1 are aware of and comply with their duties under this of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data; and those in respect of Confidential Information
 - 2.1.7.2 are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;
 - 2.1.7.3 have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- 2.1.8 ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
- 2.1.9 ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event;
- 2.1.10 not transfer such Personal Data outside of the UK and/or the EEA unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
 - 2.1.10.1 the transfer is in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 2.1.10.2 the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable)) as agreed with the non-transferring Party which could include the relevant parties entering into:
 - (a) Where the transfer is subject to the UK GDPR:
 - (i) The UK International Data Transfer Agreement (the "IDTA"), as published by the Information Commissioner's office under section 119A(1) of the DPA 2018 from time to time; or
 - (ii) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("EU SCCs"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "Addendum") as published by the Information Commissioner's Office from time to time and/or;
 - (b) Where the transfer is subject to the EU GDPR, the EU SCCs, as well as any additional measures determined by the non-transferring Party being implemented by the importing Party;
- 2.1.10.3 the Data Subject has enforceable rights and effective legal remedies;
- 2.1.10.4 the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and
- 2.1.10.5 the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data;
- 2.1.11 Each Joint Controller shall use its best endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3 DATA PROTECTION BREACH

3.1 Without prejudice to Paragraph 3.2 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:

- 3.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation;
- 3.1.2 all reasonable assistance, including:
 - 3.1.2.1 co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - 3.1.2.2 co-operation with the other Party including using such best endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Data Loss Event;
 - 3.1.2.3 co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or
 - 3.1.2.4 providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including the information set out in Paragraph 3.2 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data;.

3.2 Each Party shall use best endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event which is the fault of that Party as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular:

- 3.2.1 the nature of the Data Loss Event;
- 3.2.2 the nature of Personal Data affected;
- 3.2.3 the categories and number of Data Subjects concerned;
- 3.2.4 the name and contact details of the Party's Data Protection Officer or other relevant contact from whom more information may be obtained;
- 3.2.5 measures taken or proposed to be taken to address the Data Loss Event; and
- 3.2.6 a description of the likely consequences of the Data Loss Event.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

4 AUDIT

4.1 The Supplier shall permit:

- 4.1.1 the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data; and the Data Protection Legislation; and/or
- 4.1.2 the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data in lieu of conducting such an audit, assessment or inspection.

5 IMPACT ASSESSMENTS

5.1 The Parties shall:

- 5.1.1 provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures); and
- 5.1.2 maintain full and complete records of all processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6 ICO GUIDANCE

6.1 The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Crown Body.

7 LIABILITIES FOR DATA PROTECTION BREACH

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Data Loss Event ("Financial Penalties**") then the following shall occur:**

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 7.1.1 if in the view of the Information Commissioner, the Buyer is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Data Loss Event;
 - 7.1.2 if in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or
 - 7.1.3 if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Data Loss Event and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Data Loss Event can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in clause 36 of the Conditions (Resolving disputes).
- 7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "**Claim Losses**"):
 - 7.3.1 if the Buyer is responsible for the relevant Data Loss Event, then the Buyer shall be responsible for the Claim Losses;
 - 7.3.2 if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and
 - 7.3.3 if responsibility for the relevant Data Loss Event is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 7.4 Nothing in either Paragraph 7.2 or Paragraph 7.3 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Data Loss Event, having regard to all the circumstances of the Data Loss Event and the legal and financial obligations of the Buyer.

8 TERMINATION

- 8.1 If the Supplier is in Material Breach under any of its obligations under this of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data, the Buyer shall be entitled to terminate the Contract by issuing a termination notice to the Supplier in accordance with clause 11 of the Conditions (Ending the contract).

9 SUB-PROCESSING

- 9.1 In respect of any processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
- 9.1.1 carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
 - 9.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10 DATA RETENTION

- 10.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Part C Independent Controllers (*Optional*)

1 INDEPENDENT CONTROLLER PROVISIONS

- 1.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controller.
- 1.2 Each Party shall process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
- 1.3 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 1.1 of this Part C Independent Controllers (*Optional*) of Annex 1 – Processing Personal Data above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
- 1.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the processing of Personal Data for the purposes of the Contract.
- 1.5 The Parties shall only provide Personal Data to each other:
- 1.5.1 to the extent necessary to perform their respective obligations under the Contract;
 - 1.5.2 in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects);
 - 1.5.3 where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK and/or the EEA, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
 - 1.5.3.1 the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or
 - 1.5.3.2 the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable)) as determined by the non-transferring Party which could include the parties entering into:
 - (a) where the transfer is subject to UK GDPR:
 - (i) the UK International Data Transfer Agreement (the “**IDTA**”), as published by the Information Commissioner’s Office or such updated version of such IDTA as is published by the Information Commissioner’s Office under section 119A(1) of the DPA 2018 from time to time; or

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- (ii) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (the “**EU SCCs**”), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the “**Addendum**”) as published by the Information Commissioner's Office from time to time; and/or

(b) where the transfer is subject to EU GDPR, the EU SCCs; as well as any additional measures determined by the non-transferring Party being implemented by the importing party;

1.5.3 the Data Subject has enforceable rights and effective legal remedies;

1.5.4 the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

1.5.5 the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

1.5.4 where it has recorded it in Part A Authorised Processing Template of Annex 1 – Processing Personal Data.

1.6 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1.7 A Party processing Personal Data for the purposes of the Contract shall maintain a record of its processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

1.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (“**Request Recipient**”):

1.8.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

- 1.8.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's processing of the Personal Data, the Request Recipient will:
 - 1.8.2.1 promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - 1.8.2.2 provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 1.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - 1.9.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;
 - 1.9.2 implement any measures necessary to restore the security of any compromised Personal Data;
 - 1.9.3 work with the other Party to make any required notifications to the Information Commissioner's office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - 1.9.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 1.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Part A Authorised Processing Template of Annex 1 – Processing Personal Data.
- 1.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Part A Authorised Processing Template of Annex 1 – Processing Personal Data.
- 1.12 Notwithstanding the general application of clauses 14.9 to 14.9.13 of the Conditions to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 1.1 to 1.12 of this Part C Independent Controllers (*Optional*) of Annex 1 – Processing Personal Data.

[Annex 2 – Specification]

The TPAP Audit requires the physical examination of a third party's security controls at their relevant sites. The audit is undertaken in accordance with police national physical security policies and standards, whilst incorporating the latest advice from the National Physical Security Authority.

Audits include written recommendations which are provided to the third party, where appropriate, to improve security.

Reports are then provided to the relevant Home Office delivery team, alongside other output from assessments undertaken via the TPAP tooling, which are then used to inform the risk owner.

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

[Annex 3 – Charges]. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

VI. Annex 4 – Supplier Tender – NOT USED

Crown Copyright 2023

Cyber Security Assessments for Third Parties seeking to connect into Home Office provided police systems.

VII. Annex 5 – Optional IPR Clauses – NOT USED