SUPPLEMENTAL GDPR CLAUSES TO ANY EXISTING AGREEMENT BETWEEN CACI LIMITED AND ITS CLIENTS.

These Supplemental GDPR Clauses shall apply from 25 May 2018 between CACI Limited (CACI) and its clients.

Recitals

(A) These Supplemental GDPR Clauses shall apply to any existing written agreement between CACI and its clients where CACI is required to Process Personal Data on behalf of it clients and there are no other agreed written GDPR compliant data processing clauses nor a GDPR compliant data processing agreement between the parties.

(B) These Supplemental GDPR Clauses are intended to cover all of the minimum requirements under GDPR and some additional clauses (i.e. clauses 3 – 5 below), but otherwise do not alter any other agreed terms between us that do not relate to or are not associated with data protection (i.e. the non-data privacy related terms and conditions remain unchanged in the Agreement).

Definitions:-

The following capitalised terms used in these Supplemental GDPR Clauses shall have the meaning set out in GDPR (e.g. in Article 4) as applicable; Controller, Data Subject, Processor, Processing (and Process and Processed shall be construed according to this definition of Processing), Personal Data, Personal Data Breach, Supervisory Authority (e.g. The Information Commissioner).

Agreement: means the current written agreement(s) between the parties pursuant to which Personal Data is being Processed.

Data Protection Officer: means Raj Afghan, at CACI Limited, CACI House, Kensington Village, Avonmore Road, London W14 8TS (email: DPO@caci.co.uk) or such other persons as notified to the Controller from time to time.

GDPR: means the General Data Protection Regulation (EU) 2016/679), or any successor legislation enforce in the UK and in either case as amended and/or updated from time to time.

Law: means the laws of England and Wales.

1. General

1.1 The parties agree that:

1.1.1 the Supplemental GDPR Clauses are incorporated into the Agreement and shall replace the data protection clauses entered into between the parties that relate to the Data Protection Act 1998 and/or do not comply with GDPR;

1.1.2 if there is any conflict or inconsistency between the Supplemental GDPR Clauses and the terms and conditions in the Agreement that relate to the Processing and confidentiality of Personal Data, the provisions of the Supplemental GDPR Clauses shall prevail.

1.1.3 these Supplemental GDPR clauses only apply where CACI is the Processor under the Agreement and the client is the Controller.

2. Article 28 GDPR compliant clauses

Details about the processing

2.1 The parties agree that the Agreement, includes the following details about the Processing:

2.1.1 the subject matter and duration of the processing of the Personal Data.

2.1.2 the nature and purpose of the Processing of the Personal Data.

2.1.3 the types of Personal Data to be Processed.

2.1.4 the categories of Data Subjects to whom the Personal Data relates.

However, if for any reason the above details are not set out in the Agreement then the parties shall complete Annex 1 and agree in writing that it applies to these Supplement GDPR Clauses.

Written Instructions

2.2 The Processor will only Process Personal Data in accordance with the Controller's written instructions unless the Processor is required to act without such written instructions by Law.

Confidentiality

2.3 The Processor will ensure that only the Processor's employees, consultants, directors and officers who need to Process the Personal Data under the Agreement shall have access to it and provided that in each case they have prior entered into a written agreement with the Processor that contains an obligation that such employees, consultants, directors and officers are obligated to keep information (including Personal Data) made available to them confidential.

Security

2.4 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks relating to its Processing of the Personal Data and in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data transmitted, stored or otherwise Processed. The Processor agrees to use the appropriate technical and organisational measures set out in the Agreement or where these are inadequate to use those set out in Annex 2.

Using sub-processors

2.5 The Processor shall not employ any sub-processor(s) without the prior specific or general written authorisation of the Controller. The Processor must notify the Controller of any changes it intends to make to the agreed sub-processor(s) and give the Controller a reasonable opportunity to object to such changes. The Processor shall enter into a written contract with each sub-processor which contains the same or substantially the same data protection obligations on the sub-processor as set out in these Supplemental GDPR Clauses. The Processor agrees that it shall be fully liable to the Controller for performance of the sub-processor(s) obligations as required under GDPR and the contract entered into between the Processor and sub-processor.

Data Subjects' rights

2.6 The Processor shall, subject to taking into account the nature of the Processing it carries out and by having appropriate technical and organisational measures in place, assist the Controller upon request to fulfil its obligations that relate to enabling Data Subjects to exercise their rights under GDPR, such as subject access requests, requests for rectification or erasure of Personal Data and making objections to Processing,

Assisting the Controller

2.7 The Processor shall, subject to taking into account the nature of the Processing it carries out and the information available to it, assist the Controller upon request in meeting its obligations under GDPR (i.e. under Articles 32 to 36) relating to:

2.7.1 keeping the Personal Data secure;

2.7.2 notifying Personal Data Breaches to the Supervisory Authority (in particular the Processor agrees to notify Controller as soon as reasonably practicable upon receipt of any communication, notice, request or complaint from a Data Subject; and notifying the Controller of any Personal Data Breach without undue delay once the Processor becomes aware of the breach and providing the Controller with such reasonable assistance and information in relation to such Personal Data Breach as the Controller requests);

2.7.3 advising the Data Subjects when there has been a Personal Data Breach;

2.7.4 carrying out data protection impact assessments ("DPIA"); and

2.7.5 consulting with the Supervisory Authority where the DPIA indicates there is an unmitigated high risk to the processing.

Return/deletion of Personal Data at the end of the Agreement

2.8 Unless required by Law to retain the Personal Data, the Processor shall upon termination or expiry of the Agreement, at the Controller's choice, either delete or return to the Controller all of the Personal Data it has been Processing for the Controller.

Audits and Inspections

2.9 The Processor shall in relation to the Processing it carries out:

2.9.1 provide the Controller with all the information that is needed show that the Processor has met all of its obligations under these Supplemental GDPR Clauses;

2.9.2 at the Controller's request submit and contribute to audits and inspections that the Controller or the Controller's appointed auditor carries out;

2.9.3 pursuant to Article 28.3(h) immediately inform the Controller if, in its opinion, it has been given an instruction which does not comply with the GDPR.

Controller's obligations

2.10 The Controller shall comply with its obligations under GDPR including in relation to its collection, processing and provision of Personal Data to the Processor in connection with the Agreement.

Additional Clauses

3. Overseas transfers

The Processor shall not transfer the Personal Data to any country or international organisation located outside the European Economic Area ("EEA") or, in the event the UK ceases to be a member of the EEA, outside the UK without the prior written consent of the Controller.

4. Processor's other obligations

In addition to these Supplemental GDPR Clauses the Processor has direct obligation under GDPR which the Processor agrees to comply with to the extent applicable (i.e. those obligations set out in Articles 27, 29, 30.2, 31, 32, 33 and 37). The Processor agrees that it has appointed a Data Protection Officer.

5. Liability

The Processor shall be liable to the Controller for any losses, damages and costs (including reasonable legal costs) arising from the Processor's breach of Supplemental GDPR clauses subject to Article 82 of GDPR and any limitations in the Agreement. The Processor shall only be liable for any payment to the Controller resulting from its breach of these Supplemental GDPR Clauses to the extent that such payment has been ordered by a competent court in the UK, a legally binding decision of the Supervisory Authority or other regulatory body in the UK, or by way of a written agreement between the Controller and Processor after the breach arises.

Annex 1

Details relating to the Personal Data and Processing pursuant the Agreement.

The subject matter and duration of the processing of the Personal Data.	
The nature and purpose of the processing of the Personal Data.	
The types of Personal Data to be processed.	
The categories of Data Subjects to whom the Personal Data relates.	
The obligations and rights of the Controller.	**As set out in above and/or in the Agreement.**
State the names of any subprocessors and confirm if a GDPR compliant data processing agreement has been entered into with such sub-processor.	

Annex 2

Details of technical and organisational security measures to protect the Personal Data and the Processing of such data.

CACI shall use the technical and organisational security measures required under its ISO270001 accreditation.

In particular, as part of CACI's ISO27001 accreditation CACI maintains internal policies and procedures which are designed to:

(a) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(b) has back-up, archive and/or disaster recovery processes which are capable of restoring the availability and access; to Personal Data in a timely manner in the event of a physical or technical incident; and

(c) minimise security risks, including through regular security risk assessment, evaluation and testing.