National Communications Data Service (NCDS)

Information Assurance Service

Homeland Security Group

2 Marsham Street, London SW1P 4DF

Tel: +44 (0)20 7035 4848

www.homeoffice.gov.uk

Supplier Security Manager:

……

Address:

……

……

……

Date: ……..

SUBJECT: SECURITY ASPECTS LETTER (SAL) FOR PARTICIPATION IN THE MARKET ENGAGEMENT STAGE OF THE NEXT GENERATION CONTRACT(S) PROJECT

1. This letter sets out certain security provisions which ……. (the **Supplier)** must comply with when participating in all Market Engagement activities in relation to the Next Generation Contract(s) Project in support of the Home Office (the **Authority)**

2. This letter sets out certain security provisions which the **Supplier** must comply with when providing support to the **Authority.** It explains the **Supplier** responsibilities when dealing with Her Majesties Government (HMG) information assessed as OFFICIAL or OFFICIAL SENSITIVE in accordance with the Government Security Classifications policy, April 2014.

3. The Authority intends to disclose information (the Confidential Information) to the Supplier for the **Purpose** of testing the **Authority** requirements and approaches for procurement of Management & Advisory Services and Enabling DDaT Capabilities as set in Procurement Information Notice titled ‘Home Office Next Generation Contract(s)’.

4. The Supplier undertakes not to use the Confidential Information for any purpose except the **Purpose,** without first obtaining the written agreement of the Authority.

5. The Recipient undertakes to keep the Information secure and not to disclose it to any third party [except to its employees [and professional advisers] who need to know the same for the Purpose, who know they owe a duty of confidence to the Discloser and who are bound by obligations equivalent to those in Clause 2 and Clause 3 as above.

6. Data which is entrusted to the **Supplier** and its employees must be protected by the **Supplier** and its employees in accordance with the requirements contained within the Home Office Services Security Policy v0.6, at Annex B. The **Supplier** shall ensure that a SAL on equivalent terms to this SAL shall be entered into by the **Supplier** and the relevant subcontractor.

7. For the avoidance of doubt any reference in this SAL to "Employee" means any of the **Supplier** employees, agents, officers, directors, secretaries or 3rd Party Suppliers providing support to the **Purpose.**

8. The **Supplier** should consult with the NCDS Commercial team immediately where any doubt exists as to the protection necessary to safeguard any classified material.

9. The **Supplier** shall report immediately to the Home Office Departmental Security Officer, via the NCDS Information Assurance Service, any incident or information that raises doubts as to compliance with the terms of this SAL.

10. All information provided by the **Authority** shall be marked as OFFICIAL or OFFICIAL SENSITIVE. In the event that a document or information is unmarked it must be treated as OFFICIAL.

11. All HMG information has a value so the terms NOT CLASSIFIED or NPM must NOT be used. HMG information (whether marked or unmarked) must be treated as a minimum of OFFICIAL.

12. The caveat SENSITIVE is applied to indicate that the compromise of the information potentially has the following serious impacts:

Impact Statements
An individual's personal safety or liberty is put at risk
The detection or investigation of serious crime is hindered, impeded or impaired or a serious crime is facilitated.
The collapse of one or more criminal prosecutions or a number of criminal convictions being declared unsafe or referred for appeal.

A unique Security Intelligence Agency or National Crime Agency intelligence operation is halted or damaged or cause damage to a UK or allied intelligence capability.
Financial loss of up to £100 million to HMG or the Public Sector.
Any individual suffers severe or devastating financial loss or a large company or a number of small businesses are lost.
There is a loss of control of an individual's or large group of individual's sensitive data e.g. call record information.
There is a breach of an individual's expectation of privacy under Data Protection legislation.
NCDS or the Home Office suffers short-term reputational damage or there is unplanned parliamentary scrutiny of the programme or the programme is the subject of a few days adverse coverage in national or specialist press
A Telecommunications Operator (TO) suffers short-term reputational consequences or is subject to unplanned scrutiny by the Stock Market, Department of Trade, and Industry (DTI) or other Financial Regulator or is the subject of a few days of adverse coverage in national or specialist press.
There is unplanned expenditure to defend the reputation of HMG, the Home Office, The **Authority**, a Partnership/Authority stakeholder or a TO.
An actual, potential, or suspected reportable error or breach of Regulation of Investigatory Powers (RIPA) 2000 resulting in a breach report to the Interception of Communications Commissioner.

Table 1: Impact Statements for CCD Information

13. Communications Data, as defined by section 21(4), (6) and (7) of RIPA 2000 is OFFICIAL SENSITIVE information that must be handled in accordance with the guidance provided at Annex A. By virtue of Malone v UK (1984) European Human Rights Reports 14 Communications Data are covered by the notion of private life and correspondence under Article 8 European Court of Human Rights. It follows that Communications Data are considered personal information under the Data Protection Act (DPA)1998.
14. Where certain specific stakeholders are identified, or current or future capability gaps are described, these documents will attract a higher classification. Should the **Supplier** be required to handle or process information that is classified SECRET or TOP SECRET the **Supplier** must contact NCDS Information Assurance Service before they knowingly accept receipt of such information.

15. All non- European Economic Area (EEA) (plus Switzerland) nationals intending to participate in work relating to the **Purpose** must provide their security clearance details to the Home Office NCDS Security Officer, via the NCDS Commercial team for verification.

16. Documents that are issued to the **Supplier** with a caveat of 'UK Eyes Only (UKEO)' [1]must not be accessed or viewed by any member of staff who has a restriction on their clearance preventing access to UKEO material.

17. The following table defines the classification requirements to apply to a non-exhaustive list of aspects relating to the **Purpose.** Some aspects have specific classifications and in these cases the minimum and maximum markings will be the same; however, other aspects may span a range of markings depending on a number of factors, e.g. level of detail. More details regarding the classification requirements is available in the notes below. There may well be exceptional cases in which classifications outside the minimum and maximum markings listed in the table apply.

ASPECT (Non Exhaustive)	CLASSIFICATION Non-sensitive content	CLASSIFICATION Sensitive content
Requirements	OFFICIAL	OFFICIAL SENSITIVE
Code	OFFICIAL	OFFICIAL SENSITIVE
Defects	OFFICIAL	OFFICIAL SENSITIVE
Testing Plans	OFFICIAL	OFFICIAL SENSITIVE
High Level Designs	OFFICIAL	OFFICIAL SENSITIVE
Low Level Designs	N/A	OFFICIAL SENSITIVE
Deployment Plan	OFFICIAL	OFFICIAL SENSITIVE

[1] The United Kingdom use "Eyes Only" to indicate specific countries with whom a document may be shared. "UK Eyes Only, " for example, means that the document is only distributed within the UK and not to other countries

ASPECT (Non Exhaustive)	CLASSIFICATION Non-sensitive content	CLASSIFICATION Sensitive content
On boarding Plan	OFFICIAL	OFFICIAL SENSITIVE
Service Design	OFFICIAL	OFFICIAL SENSITIVE
Test Strategy	OFFICIAL	OFFICIAL SENSITIVE
Security Architecture Design	N/A	OFFICIAL SENSITIVE
Accreditation Plan	OFFICIAL	OFFICIAL SENSITIVE
Risk Management & Accreditation Document Set	OFFICIAL	OFFICIAL SENSITIVE
Service Management Documentation (Tickets, alerts etc)	OFFICIAL	OFFICIAL SENSITIVE
Project Plan	OFFICIAL	OFFICIAL
DLCM Lifecycle Plan	OFFICIAL	OFFICIAL
Quality Plan	OFFICIAL	OFFICIAL
Communications Plan	OFFICIAL	OFFICIAL
Risk & Opportunity Plan	OFFICIAL	OFFICIAL
Configuration Management Plan	OFFICIAL	OFFICIAL SENSITIVE
Configuration Management Database	OFFICIAL	OFFICIAL SENSITIVE
Software Development Plan	OFFICIAL	OFFICIAL SENSITIVE

ASPECT (Non Exhaustive)	CLASSIFICATION Non-sensitive content	CLASSIFICATION Sensitive content
Environment Specification	OFFICIAL	OFFICIAL SENSITIVE
Test Harness Specification	OFFICIAL	OFFICIAL SENSITIVE
Lockdown Plan	OFFICIAL	OFFICIAL SENSITIVE
SPOC PIN Database	N/A	OFFICIAL SENSITIVE
CD related Documents	N/A	OFFICIAL SENSITIVE
Cell Site Data	N/A	OFFICIAL SENSITIVE
Radio Frequency Survey Data	N/A	OFFICIAL SENSITIVE
Communication Solution Provider (CSP) Contact Database	OFFICIAL	OFFICIAL
Authorised request for Communication Data (CD)	N/A	OFFICIAL SENSITIVE
Authorised response to a CD request	N/A	OFFICIAL SENSITIVE
CDLI/DCCU/NCDS Vision Statements	TBC	TBC
Operating Model CDLI Partnership		OFFICIAL SENSITIVE
Target Operating Model NCDS		OFFICIAL SENSITIVE

ASPECT (Non Exhaustive)	CLASSIFICATION Non-sensitive content	CLASSIFICATION Sensitive content
Investment Plan/Portfolio		OFFICIAL SENSITIVE

Table 2: Detailed schedule of classification

Notes

- Where the classifications above differ for a particular aspect this is indicative that the precise sensitivity and detail of the aspect should be taken into account. It is the responsibility of the **Supplier** security lead to ensure that the appropriate classification is correctly applied at each issue.
- Where a document is supplied to the **Supplier** by the **Authority** with an existing protective marking or classification that classification or marking may not be changed and no extract from that document may be added to a document at a different classification without the permission of the author of the document.
- It should be noted that the classifications apply to the aspects taken in isolation. Where there is association between two or more aspects, then the guidance would be to consider that the aspect is more sensitive and use the SENSITIVE caveat accordingly.

18. This includes aggregation by accumulation and association.

19. There may be occasions when Supplier is required to communicate directly with UK Police Forces who may still have legacy information that is marked under the old Government Protective Marking Scheme.

20. Annex A contains the handling instructions and security provisions for storage and transmission which will apply to tasks in support of NCDS projects.

21. You are requested to acknowledge receipt of this letter by signing and returning the attached copy and confirm that the level of classification associated with the requirements listed in this letter has been brought to the attention of the individuals directly responsible for the provision of the various services associated with the Market Engagement stage. Additionally, confirming that the requirements are all fully

understood and that the required security controls can and will be taken to safeguard the material concerned.

22. Should you have any questions regarding this SAL or how it should be applied please contact a member of NCDS Information Assurance Service.

Yours Faithfully

Mike Purvis

Senior Information Risk Owner (SIRO)

NCDS Information Assurance Service

2 Marsham Street, London, SW1P 4DF

NCDSIATeam@homeoffice.gov.uk

DIOCommercial@homeoffice.gov.uk

The **Supplier** acknowledges and agrees to comply with the terms of this Security Aspects Letter. It acknowledges receipt of this letter and confirms that the level of classification associated with the requirements listed in this letter have been brought to the attention of the individuals engaged on the **Purpose**. The **Supplier** also confirms that the requirements are fully understood, and that the required security controls can and will be taken to safeguard the material concerned.

Signed_____

Dated_____

Name: Position:

For and on behalf of the **Supplier**

ANNEX A

Classification – Handling Instructions

The following table defines the handling instructions that apply to material classified as OFFICIAL and OFFICIAL SENSITIVE.

Material that has an existing Protective Marking of RESTRICTED must be handled as OFFICIAL SENSITIVE.

Classification	Handling instructions
OFFICIAL	HSG policy is that OFFICIAL documents shall be marked as such. **Need to Know** • Check that the recipient can handle this material i.e. is authorised and briefed to receive information on the subject. • May only be circulated to persons authorised and briefed to receive the information. **Clearance** • Baseline Personnel Security Standard (BPSS) or Counter-Terrorist Check (CTC). • Information that is Communications Data (as defined in s21 RIPA 2000) must only be handled by persons with a minimum clearance of SC **Telephone calls** • Ensure conversations cannot be overheard **Classification** • This marking must not be removed unless there is a pre-existing agreement with the originating Department **On the move** • No information and/or assets are left unattended in a public place or motor vehicle or entrusted to an unauthorised person(s) (E.g. placing them in a hotel safe or cloakroom)
OFFICIAL	Home Office policy is that OFFICIAL SENSITIVE

SENSITIVE	documents shall be marked as such and that descriptors shall NOT be used. **Need to Know** • Check that the recipient can handle this material i.e. is authorised and briefed to receive information on the subject. • May only be circulated to persons authorised and briefed to receive the information. • Circulation to persons who have not been approved or briefed must be approved by the originator and then only on a case by case basis. All such circulations must be recorded and made available for audit by the Authority. • Information must not be shared outside secure government channels (For example PNN and CJSM) without a pre-existing agreement relating to this information or reference to the originating body in advance of sharing. **Clearance** • Baseline Personnel Security Standard (BPSS) or Counter-Terrorist Check (CTC). • Information that is Communications Data (as defined in s21 RIPA 2000) must only be handled by persons with a minimum clearance of SC. **Telephone calls:** • Ensure conversations cannot be overheard and use guarded speech to desensitise the information discussed.
SECRET	To be detailed if and when required

Classification - Storage

The following table defines where materials (including, without limitation, data) may be stored.

Material that has an existing Protective Marking of RESTRICTED must be handled as OFFICIAL SENSITIVE.

Classification	Storage/Disposal Arrangements
OFFICIAL	Storage Arrangements (documents):- Protected by one barrier, e.g. a locked container within a secure building. Storage Arrangements (electronic): - Refer to NCDS Information Assurance Service for guidance. Disposal of Papers: - Tear into at least four pieces or shred. Use secure waste sacks. Keep sacks secure until final disposal through a trusted disposal method. Disposal of Magnetic Media: - Securely destroy as follows: Floppy Disk - dismantle and cut disk into quarters. Compact Disc (CD)/ Digital Versatile Disc (DVD) - destroy completely - disintegrate, pulverise, melt, or shred.
OFFICIAL SENSITIVE	Storage Arrangements (documents):- Protected by two barriers, e.g. a locked container within locked office in a secure building. Storage Arrangements (electronic):- Not to be stored on corporate network without appropriate 'Need to Know' controls being put in place to limit access to authorised persons only, e.g. encrypted file store. May be stored on standalone system, arrangements for storage must be formally approved by the NCDS Information Assurance Service. Disposal of Papers: - Downgrade by tearing into small pieces and place in secure waste sacks, or use a cross cut shredder. Keep sacks secure until final disposal. Disposal of Magnetic Media: - Securely destroy - Floppy disk - dismantle and cut disk into quarters (at least), dispose with normal waste. CD/DVD - destroy completely - disintegrate, pulverise, melt or shred. OFFICIAL SENSITIVE information must be appropriately protected so that it can only be seen by

	the intended audience through access control on systems and physical measures such as secure storage
SECRET	To be detailed if and when required

Classification – Transmission

The following table defines the methods by which materials (including, without limitation, data) may be transmitted for.

Material that has an existing Protective Marking of RESTRICTED must be handled as OFFICIAL SENSITIVE.

Classification	Acceptable Methods of Transmission
OFFICIAL	Mail: - By post or courier, in a sealed envelope. Telephone: - May be used. Facsimile: - Check recipient is on hand to receive then transmit. Corporate Network: - May be used. Internet: - Refer to NCDS Information Assurance Service for guidance. Formally approved HMG networks for OFFICIAL and OFFICIAL-sensitive: - May be used.
OFFICIAL SENSITIVE	Mail: - By post or courier, in a sealed envelope. Do not show classification on the envelope. Telephone: - Public Service Telephone Network (PSTN) and digital telephones may be used. WAP telephones may not be used. Facsimile: - Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending. Corporate Network: - Must be encrypted with a

	commercial grade encryption product before being transmitted within a corporate network. Passwords must be sent to the recipient by an alternative method and not included in the email. NCDS Information Assurance Service must formally approve this transmission method. Internet: - As corporate network above. Crown Justice Systems Networks: - May be used to send material to CJSM email addresses. OFFICIAL SENSITIVE information must be appropriately protected so that it can only be seen by the intended audience through access control on systems and physical measures such as secure storage. The Partnership will only communicate by email with Suppliers who have adopted NCSC Guidance for Secure Email. Your service must be capable of sending and receiving email using Transport Layer Security (TLS) 1.2 or 1.3 or via CJSM.
SECRET	To be detailed if and when required