

Framework Schedule 9 (Cyber Essentials Scheme)

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (*Definitions*):

"Cyber Essentials Scheme"	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found at: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview ;
"Cyber Essentials Basic Certificate"	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
"Cyber Essentials Certificate"	a Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate or a written statement that equivalent controls are in place through other means, verified by a technically competent and independent third party which must be an Information Assurance for Small and Medium Enterprises (IASME) registered certification body to be provided by the Supplier as set out in the Framework Award Form;
"Cyber Essential Scheme Data"	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
"Cyber Essentials Plus Certificate"	the certification awarded on the basis of external testing by an independent certification body of the Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. What Certification do you need

- 2.1 Where the Framework Award Form requires that the Supplier provide a Cyber Essentials Certificate prior to **[Category Guidance: add**

appropriate wording with respect to status of contract to be agreed with Sourcing. All Paragraphs must be reviewed to ensure that the wording added is consistent with all other Paragraphs in the Schedule] the Supplier shall provide a valid Cyber Essentials Certificate

to CCS. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under any Contract until such time as the Supplier has evidenced to CCS its compliance with this Paragraph 2.1.

- 2.2 Where the Supplier continues to Process Cyber Essentials Scheme Data during the Contract Period of any Call-Off Contract the Supplier shall deliver to CCS evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.
- 2.3 Where the Supplier is due to Process Cyber Essentials Scheme Data after the Start Date of the first Call-Off Contract but before the end of the Framework Contract Period or Contract Period of the last Call-Off Contract, the Supplier shall deliver to CCS evidence of:
 - 2.3.1 a valid and current Cyber Essentials Certificate before the Supplier Processes any such Cyber Essentials Scheme Data; and
 - 2.3.2 renewal of the valid Cyber Essentials Certificate on each anniversary of the first Cyber Essentials Scheme certificate obtained by the Supplier under Paragraph 2.1.
- 2.4 In the event that the Supplier fails to comply with Paragraphs 2.2 or 2.3 (as applicable), CCS reserves the right to terminate the Contract for Material Default and the consequences of termination in Clause 13.4.1 of the General Terms shall apply.
- 2.5 The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Scheme Data require the Subcontractor to provide a valid Cyber Essentials Certificate, at the equivalent level to that held by the Supplier. The Supplier cannot require the Subcontractor to commence the provision of Deliverables under the Sub-Contract until the Subcontractor has evidenced to the Supplier that it holds a valid Cyber Essentials Certificate.
- 2.6 This Schedule shall survive termination or expiry of the Contract and each and any Call-Off Contract.

