DCPP
Defence Cyber
Protection Partnership

Guidance

Cyber Essentials Scheme: Requirements for suppliers

January 2017

Introduction

Cyber Essentials is the government-backed and industry-supported scheme to guide businesses in protecting themselves against cyber threats.

The scheme is a key element of the UK's National Cyber Security Programme. Cyber Essentials certification is available to all organisations, of all sizes, and in all sectors.

Defence Cyber Protection Partnership

The Ministry of Defence (MOD) has implemented Cyber Essentials as part of the Defence Cyber Protection Partnership (DCPP) and the Cyber Security Model (CSM) which is applied to every new MOD requirement.

This guide is for defence suppliers and other DCPP stakeholders; it introduces the Cyber Essentials Scheme, outlines its role in the CSM, and how suppliers can achieve certification.

Contents

What is the Cyber Essentials Scheme?

Cyber Essentials is the recognised baseline standard for cyber security, developed by HM Government.

The scheme was developed by government to provide a clear statement of basic controls which all organisations can implement, and use to demonstrate these essential precautions to customers and other stakeholders.

Under the scheme, organisations can apply for a badge which recognises their achievement of this nationally-recognised standard. There are two levels of certification:

Cyber Essentials

Organisations complete a self-assessment questionnaire and the responses are independently reviewed by an external certifying body.

Cyber Essentials Plus

This covers the same requirements as Cyber Essentials but tests of the systems are carried out by an external certifying body, using a range of tools and techniques.

Cyber Essentials Assurance Framework

The Cyber Essential scheme sets out five security controls that are designed to prevent ‘around 80% of cyber attacks’. By achieving certification, organisations can demonstrate to customers and other stakeholders that they have taken these essential precautions.

1. Boundary firewalls and internet gateways - these are devices designed to prevent unauthorised access to private networks. Good setup of these devices either in hardware or software form is important for them to be fully effective.

2. Secure configuration - ensuring that systems are configured in the most secure way for the needs of the organisation.

3. Access control - ensuring that only those who should have access to systems have access and at the appropriate level.

4. Malware protection - ensuring that virus and malware protection is installed and that it is up-to-date.

5. Patch management - ensuring the latest supported version of applications are used and all the necessary patches supplied by the vendor have been applied.

Requirements for Ministry of Defence suppliers and sub-contractors

The Ministry of Defence (MOD) is committed to ensuring Defence and its supply chain are appropriately protected from the cyber threat.

The Defence Cyber Protection Partnership (DCPP) includes Cyber Essentials within its Cyber Security Model (CSM) as a proportionate means for suppliers to demonstrate baseline security controls. The CSM applies to all MOD contracts and suppliers will be required to demonstrate that they have achieved the appropriate level of certification.

Requirements for 'Very Low' risk contracts

The following requirements apply to all suppliers bidding for MOD contracts which have been categorised by Risk Assessment as Very Low risk:

Suppliers must hold valid Cyber Essentials certification;

- by the contract start date;
- and, this must be renewed annually;
- The scope of the certification should cover the supplier's relevant operations and network boundary which will be used to deliver the MOD contract.

Requirements for 'Low', 'Moderate' and 'High' risk contracts

The following requirements apply to all suppliers bidding for MOD contracts which have been categorised by Risk Assessment as Low, Moderate or High risk:

Suppliers must hold valid Cyber Essentials PLUS certification;

- by the contract start date;
- and, this must be renewed annually;
- The scope of the certification should cover the supplier's relevant operations and network boundary which will be used to deliver the MOD contract.

Requirements for sub-contactors

For contracts of Moderate or High risk, any elements of the work that are sub-contracted by the winning bidder(s) are subject to the Cyber Essentials requirements outlined above.

How to achieve Cyber Essentials

The Cyber Essentials scheme has been designed in consultation with a range of organisations, including SMEs, to be light-touch and to make certification achievable at a low cost. The information below outlines how to achieve Cyber Essentials or Cyber Essentials PLUS certification.

How does certification work?

Cyber Essentials can be be achieved using an online self-assessment which measures an organisation against the five security controls (see pg. 5). The self-assessment is then independently verified by an Assessor.

Cyber Essentials PLUS is achieved using the same self-assessment questionnaire, however the organisation is then subject to more comprehensive range of system testing, by an independent Assessor.

A number of Accreditation Bodies are authorised to offer Cyber Essentials certification, through the appointment of Certifying Bodies.

Each Accreditation Body can provide further information and guidance about their services and products. Visit cyberaware.gov.uk or more information.

Scope of Cyber Essentials certification and security controls

The Cyber Essentials scheme represents a small yet essential part of defending against cyber threats. It does not present all of the security controls an organisation needs to have in place to protect against a broad range of threats, particularly those that are sophisticated threats (i.e. a threat with significant capability, funding and resource, typically known as advanced persistent threats).

Useful links

The following links provide supporting information and guidance about the Cyber Essentials scheme and its role in the DCPP Cyber Security Model.

About Cyber Essentials:

Cyber Aware
https://www.cyberaware.gov.uk/cyberessentials/
The official Government site for information and guidance on the Cyber Essentials scheme.

National Cyber Security Centre
https://www.ncsc.gov.uk/
Find out more about Cyber Essentials in the context of the national cyber security strategy.

HMG Cyber Essentials Assessment
(via The Supplier Registration Service for Government)
https://sid4gov.cabinetoffice.gov.uk/
Take the online assessment and gain your Cyber Essentials certification.

About DCPP:

DCPP Information
https://www.gov.uk/government/collections/defence-cyber-protection-partnership
Guidance and supporting materials about DCPP and the Cyber Security Model, for MOD suppliers, sub-contractors and Project Teams.

Cyber Essentials requirements for public sector suppliers:

Industry Security Notice 2016/01: MOD Implementation of Cyber Essentials Scheme
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/494608/ISN_2016-01_Implementation_of_Cyber_Essentials_Scheme-O.pdf
The ISN setting out MOD's requirement from January 2016 for suppliers of contracts involving 'MOD identifiable information' to achieve Cyber Essentials Scheme certification.

Procurement Policy Note 09/14: Cyber Essentials scheme certification
https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification
The Policy Note outlining the mandatory requirement for all central government contracts which involve ICT products and services, and/or the handling of personal information.