Crown Commercial Service

Procurement Policy Note – Cyber Essentials Scheme

Action Note 09/14 25/May 2016

Issue

1. PPN 09/14 pointed to steps Government was taking to further reduce the levels of cyber security risk in its supply chain. In consultation with industry Government developed the Cyber Essentials Scheme (referred to throughout this document as Cyber Essentials). Cyber Essentials is for all organisations, of all sizes, and in all sectors. Government widely encourages its adoption and made it mandatory for Central Civil Government contracts advertised after 1 October 2014 which feature characteristics involving handling of personal information and provision of certain ICT products and services. Details are set out in Annex A.

2. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

3. Cyber Essentials covers the basics of cyber security in an organisation's enterprise or corporate IT system. There are two levels of certification – Cyber Essentials and Cyber Essentials Plus. Cyber Essentials Plus is more rigorous as it requires vulnerability tests to be performed as part of the certification.

4. MOD was not included in the original scope of PPN 09/14 on the basis it planned to mandate its own Cyber Security Model (CSM) for all new contracts from early 2015. However MoD has subsequently asked to be brought into the scope of this policy, and apply to new contracts from the date hereof. This updated PPN implements that change and supersedes PPN 09/14 although the remainder of the content of PPN 09/14 is otherwise unchanged.

Dissemination and Scope

5. The contents of this Procurement Policy Note ("PPN") apply to all Central Government Departments including Non-Ministerial Departments, Executive Agencies and Non-Departmental Public Bodies including MoD ("in-scope organisations"). Please circulate this

document within your organisation, drawing it to the attention of those with a purchasing role.

6. Other contracting authorities (e.g. in local government and the wider public sector) may choose to apply the measures set out in this PPN.

7. Private sector organisations can also apply Cyber Essentials in their dealings with private sector supply chain providers

Timing

8. This PPN applies to relevant procurements advertised after the date hereof.

Action

9. In-scope organisations must apply the requirements set out in Annex A to relevant procurements. Relevant procurements are defined at paragraph 2 of Annex A. A series of links are provided at Annex B and FAQs are provided at Annex C.

Background

11. Two levels of certification are available:

- Cyber Essentials certification is awarded on the basis of a validated self- assessment. An organisation undertakes their own assessment of their implementation of the Cyber Essentials control themes via a questionnaire, which is approved by a senior executive such as the CEO. The questionnaire is then verified by an independent Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded. This option offers a basic level of assurance and can be achieved at low cost.
- Cyber Essentials Plus offers a higher level of assurance through the external testing of the organisation's cyber security approach. Cyber Essentials Plus comprises remote and on site vulnerability testing to check whether the controls claimed actually defend against basic hacking and phishing attacks. It is therefore the more rigorous assessment and should be used when risk is assessed as higher. Given the more resource intensive nature of this process, it is likely that Cyber Essentials Plus will cost more than the foundation Cyber Essentials certification.

12. Cyber Essentials was developed by Government and industry to fulfil two functions. Firstly it provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the Government's 10 Steps to Cyber Security. Secondly through the Cyber Essentials Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

13. Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. Government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is

not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does do is define a focused set of controls which will provide cost-effective, basic cyber security for organisations of all sizes.

14. The Cyber Essentials Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, was designed in consultation with SMEs, including the Federation for Small Business, to be 'light-touch' and achievable at low cost. The two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It is important to recognise that certification only provides a snapshot of the cyber security of the organisation at the time of assessment, while maintaining a robust cyber security stance requires additional measures such as a sound risk management approach, as well as on-going updates to the Cyber Essentials control themes, such as patching. This scheme offers the right balance between providing additional assurance of an organisation's commitment to implementing cyber security to third parties, while retaining a simple and low cost mechanism for doing so.

Annexes

A. Overview of key Cyber Essentials Scheme requirements

B. Useful links

C. Frequently asked questions

Contact

10. Enquiries relating to this PPN should be should be directed to the Crown Commercial Service Helpdesk on 0345 410 2222 or email info@crowncommercial.gov.uk

ANNEX A – Overview of key Cyber Essentials Scheme requirements

1. It is mandatory for suppliers to demonstrate that they meet the technical requirements prescribed by Cyber Essentials for those contracts featuring any of the characteristics set out in paragraph 2 below, less those exemptions listed at paragraphs 9-12. The requirements can be found at:

https://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf

2. Any of the following characteristics will necessitate the requirements prescribed by Cyber Essentials:

i) Where personal information of citizens, such as home addresses, bank details, or payment information is handled by a supplier.
ii) Where personal information of Government employees, Ministers and Special Advisors such as payroll, travel booking or expenses information is handled by a supplier.
iii) Where ICT systems and services are supplied which are designed to store, or process, data at the OFFICIAL level of the Government Protective Marking scheme.

3. In addition to the above Cyber Essentials could also be used in any category of Government procurement on a case-by-case basis if a contracting authority considers this appropriate. Such a use requires that a cyber security risk is identified which would not be managed by any of the existing security requirements and where the use of Cyber Essentials is a relevant and proportionate way to manage this. Examples could include:

i) Where data is held or accessed outside of the UK/EC
ii) Where data is subject to the US-EU Safe Harbor process
iii) Where data is regularly held in a separate Disaster Recovery location
iv) Escrow and Disaster Recovery suppliers with access to customer data

4. The contracting authority must select either Cyber Essentials or Cyber Essentials Plus standards for suppliers depending upon the level of assurance required. It should be noted that Cyber Essentials was developed because neither ISO27001 nor other considered standards were sufficiently prescriptive to defeat common internet based threats. In some higher risk procurements it is likely that Cyber Essentials Plus will not provide sufficient assurance on its own and additional, broader, security requirements will be specified, e.g. ISO27000 series.

5. These types of contract are likely to be from the following categories of supplier:

i) Professional services – this includes commercial, financial, legal, HR and business services (who handle data).
ii) ICT – IT Managed or Outsourced services and ICT Services (who run systems that store data).

6. As a guide to how the policy should be applied, the following contract examples would be judged to be in scope:

i) Curriculum vitae writing services to support over 1,000 individuals back into the labour market. Data held by the supplier will include name, address, telephone number, date of birth, email address and National Insurance number.

ii) Car hire services for ten thousand members of staff. Data held by the supplier will include name, work address, work email, home address (optional) and driving licence number.

iii) Contact centre services for advice, guidance and signposting over 100,000 individuals. Data held by the supplier will include name, address, postcode, telephone number, National Insurance number and limited financial details.

7. Conversely, the following contract examples would be judged to be out of scope:

i) Communications and marketing planning services for a specific departmental product or service which would not require access to personal data.

ii) Driving instructor services for 10 individuals with very limited access to personal data involved and delivered by a sole trader whose use of IT is limited and incidental to the service being delivered.

Exemptions

8. Under the detailed circumstances that follow at paragraphs 9-12 it is not necessary to apply the requirements specified under Cyber Essentials for procurements which are otherwise in scope.

9. The Government Digital Service is responsible for the management of a number of schemes which already include comprehensive cyber security obligations. Suppliers operating under the following schemes are therefore exempt from having to conform to the requirements of Cyber Essentials:

i) G-Cloud: Cloud services procured through G-Cloud are assessed against Government's Cloud Service Security Principles.

ii) Digital Services Framework (DSF): DSF suppliers have been technically and commercially evaluated to provide a comprehensive choice for agile projects.

iii) Public Sector Network (PSN): PSN services are currently accredited against the network's security standards. In the future, PSN services will be assessed against Government's Network Security Principles.

iv) ID Assurance Framework: Being able to provide your identity online easily, quickly and safely is recognised as a key enabler of internet use by the Government and its users. Providers of public services such as national and local governments, major internet companies, online retailers, banks and others have to address business and security issues around identity proofing and username/password fallibility to mitigate the financial and administrative implications of identity fraud and compromise of personal data.

v) Assisted Digital: Assisted Digital is support for people who can't use online services independently.

10. Suppliers conforming to the ISO27001 standard where the Cyber Essentials requirements, at either basic or Plus levels as appropriate, (see paragraph 1 above) have been included in the scope, and verified as such, would be regarded as holding an equivalent standard to Cyber Essentials. Therefore suppliers in this situation are exempt, provided that the certification body (likely to be a consultancy) carrying out this verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies.

11. Procurements that follow the requirements outlined in the Supplier Assurance Framework and during this process fully cover Cyber Essentials requirements. The Supplier Assurance Framework is at

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255915/Supplier_Assurance_Framework_Good_Practice_Guide.pdf.

Accordingly such procurements are exempt from having to separately undertake Cyber Essentials.

12. Contracts may be exempt where use of Cyber Essentials can be demonstrated to be either not relevant or clearly disproportionate, such as where a cyber security risk is assessed as very low. In such cases it is suggested that a decision audit trail is recorded.

ANNEX B – Useful links

1. Cyber Essentials website providing further details:

www.cyberstreetwise.com/cyberessentials

2. Cyber Essentials Common questionnaire and Cyber Essentials Plus common test specification:

http://www.cesg.gov.uk/servicecatalogue/cyber-essentials/Pages/Scheme-Library.aspx.

These are the default questions and tests to be applied by certification bodies, unless an alternative arrangement has been agreed with CESG through their accreditation body.

3. Cyber Essentials Assurance Framework:

https://www.cyberstreetwise.com/cyberessentials/files/assurance-framework.pdf

4. Details of accreditation bodies are available at:

https://www.cyberstreetwise.com/cyberessentials

ANNEX C – Frequently asked questions

Q1 Why should Cyber Essentials be used in Government's supply chain?

- To manage cyber security risk in Government's supply chain
- To allow Government's suppliers to use a recognisable scheme to demonstrate to other potential customers that they take cyber security seriously; and
- It is simple, low cost to achieve and presents a minimal barrier to entry to the Government supply chain.

Q2 What technical areas does Cyber Essentials cover?

- Boundary firewalls and internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management

Q3 When should I discuss with/notify suppliers of any applicable Cyber Essentials requirement?

Ideally this should be discussed with potential suppliers in the pre-procurement stage where you are shaping your overall project requirements. Any applicable Cyber Essentials requirements must be specified in the Contract Notice under the Open procedure, and consideration should be given to highlighting any Cyber Essentials requirement in Contract Notices for other procedures to provide bidders with the longest possible time to seek certification.

Q4 How do suppliers know who to approach to undertake the certification process?

This service is provided by Government approved certification bodies which are currently accredited through the Certified Register of Ethical Security Testers (CREST), Information Assurance for Small and Medium Sized Businesses (IASME) and QG Business Solutions Ltd. Additional accreditation and certification bodies will be appointed as the Cyber Essentials Scheme develops.

Details of accreditation bodies are available at:

https://www.cyberstreetwise.com/cyberessentials

Q5 At what point is the supplier required to demonstrate possession of the Cyber Essentials certificate?

Evidence of holding a Cyber Essentials certificate (whether basic level or Plus) is desirable before contract award, but essential at the point when data is to be passed to the supplier. Under exceptional circumstances Departments may wish to make a risk-based decision and allow a contract to commence if a Cyber Essentials certification of a supplier business is either incomplete or not current.

Q6 How much will it cost a supplier to become Cyber Essentials certified?

The cost for smaller companies to be Cyber Essentials certified is expected to range between £200 and £400 at basic level, and between £1000 and £3000 at Plus level. It is possible that costs may reduce in future. Up-to-date information on costs can be found on the web pages of certification bodies, links to which can be found at

http://www.cyberstreetwise.com/cyberessentials

Q7 How often will Cyber Essentials certification need to be renewed?

Suppliers should hold a Cyber Essentials Certificate that is no more than 12 months old. As Cyber Essentials provides assurance of compliance only at the time of testing, certified organisations that do not regularly patch their ICT or do not control secure configuration may become non-compliant in substantially less than one year. The requirement to certify at more regular intervals should be risk based and determined on a case by case basis, subject to the requirements of the contract.

Q8 What does the scope of Cyber Essentials cover?

By default Cyber Essentials applies to the legal entity providing the goods/services rather than any wider corporate entity an organisation may be a part of. However organisations can reduce the scope of certification to only part of the legal entity. Conditions for this are given in the Assurance Framework at

https://www.cyberstreetwise.com/cyberessentials/files/assurance-framework.pdf

Contracting authorities should be aware that a supplier may share a client's information with a 3rd party such as a cloud service provider. Cyber Essentials does not ensure that the security of the 3rd party is in scope of certification. Contracting authorities are therefore advised to check the scope of a Cyber Essentials certificate and consider whether the risks of information sharing justify requiring Cyber Essentials certification with any 3rd party.

Q9 How does Cyber Essentials fit in with/complement existing security requirements?

- There is an existing set of information assurance and cyber security requirements that the Government has in place for suppliers. In some circumstances Cyber Essentials will be used in areas not covered by these requirements or it will be used alongside these requirements, or used as part of them.
- The Model Services Contract is a document used across Government to ensure consistency of requirements for contracts with ICT, BPO and FM providers exceeding £10 million in value. Schedule 2.4 of the Model Contract addresses security management. Within this schedule paragraph 6.1 requires that "The Supplier shall conduct relevant Security Tests from time to time." In such circumstances, where the Authority's requirements referred to in paragraph 6.1 are greater than the level of assurance provided under the Cyber Essentials or Cyber Essentials Plus, then those specific requirements will take precedence over the requirement to hold Cyber Essentials or CyberEssentials Plus. A Cyber Essentials Plus certificate would only qualify as demonstrating sufficient evidence if it covered all the Authority's requirements. However, even under those circumstances, it is possible that a

supplier could have to renew their Cyber Essentials Plus certificate several times within a 12 month period when demonstrating they comply with paragraph 6.1. The reason for this is that the Cyber Essentials Scheme provides a snapshot only and the frequency of testing is a judgement of the rate of ICT change in the organisation, confidence in the organisation to maintain patching and secure configurations, and the level of assurance required. For some contracts this may justify testing several times a year.

- The Security Policy Framework (SPF) describes the mandatory security outcomes that all Government organisations and 3rd parties handling Government information must achieve. These outcomes describe the necessary measures for information and technology, personnel and physical security. The Cyber Essentials Scheme covers some of the technical security measures.
- The ISO27001 standard is widely used but few companies who conform to this standard will automatically conform to Cyber Essentials. This is because it is not usual for all of the 5 technical controls in Cyber Essentials to be included in the scope for an ISO27001 implementation. It is also unlikely that any of these controls will have been tested as they would be under Cyber Essentials Plus. Therefore most businesses with ISO27001 will have to adopt Cyber Essentials in addition to ISO27001.
- HADRIAN is a self-assessment tool which assesses how compliant the supply chain is with Government security requirements including the SPF and Government legislation (such as the Data Protection Act). The HADRIAN tool is aligned to ISO 27001:2013. Suppliers answer questions on aspects of their security infrastructure including governance, personnel security, physical security, risk management, IT security, data handling, security training and business continuity. The results provide the user with a comprehensive and holistic understanding of the supplier's security regime and whether suppliers handle information and assets in accordance with Government security requirements. The HADRIAN question set is continually being reviewed and enhanced. The next version will have broader coverage of new and emerging risks and will include additional questions on high priority areas such as cyber defence.

Q10 Are there alternatives to demonstrating compliance with Cyber Essentials technical requirements other than through gaining the certificate?

Yes. According to EU Law a supplier is not obliged to use Cyber Essentials. A supplier need only demonstrate to the satisfaction of the contracting authority that they meet Cyber Essentials requirements. Normally this should be verified by a technically competent and independent 3rd party. To demonstrate that Cyber Essentials Plus requirements have been met it is required in all cases that verification is provided by a technically competent and independent 3rd party.

Gaining the Cyber Essentials certificate is the easiest way to demonstrate that the requirements have been met; however other forms of evidence are acceptable. Aside from

a supplier falling under one or more of the stated exemptions Cyber Essentials certification is likely to be the cheapest way to achieve this.