Cyber Essentials in the NDA

Nuclear Decommissioning Authority

IPPR01-TAC10

Rev 1 July 2016

Cyber Essentials is a government-backed, industry supported scheme that 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.

The Nuclear Decommissioning Authority (NDA) and its subsidiaries, International Nuclear Services Limited (INS) and Radioactive Waste Management Limited (RWM) are taking steps to reduce the levels of cyber security risk in its supply chain. The NDA will in future require all suppliers bidding for certain contracts, which are assessed to pose an element of information risk, to meet the requirements of the Cyber Essentials scheme. Suppliers can choose to either become Cyber Essentials certified, or will need to satisfy the NDA that they meet the requirements of Cyber Essentials through technically competent independent verification.

Cyber Essentials is not, however, typically used to assess stand-alone computers which have no connection to the internet or any other computers. Suppliers using isolated stand-alone computers must be able to demonstrate adequate security controls through the issuing of Security Operating Procedures (SyOPs), which the NDA may choose to review.

The OFFICIAL classification will contain a wide range of information of varying sensitivities and with differing consequences resulting from compromise or loss.

It is realised that not all contracts are appropriate for such assurance, and therefore we are keen not to add additional costs onto suppliers unnecessarily. However where a contract is likely to be dealing with significant volumes of personal data (payroll, hr, medical, etc.), or is likely to have a Security Aspects Letter (SAL) which covers the processing of OFFICIAL-SENSITIVE information on their own computer systems then it is appropriate to request the supplier to provide evidence that they are competent to process and store such information. In the examples above it would be necessary to request that they provide evidence that they have met the requirements of the Cyber Essentials Plus scheme.

NDA will require suppliers to demonstrably meet the technical requirements of Cyber Essentials by the contract start date, and certainly prior to any data being passed to the supplier (excluding that data which is solely tender and contracts related). Evidence of recertification or independent assurance that the supplier continues to meet the requirements of Cyber Essentials should be provided to the NDA procurement department on an annual basis.

The requirement for suppliers to demonstrate their compliance with the Cyber Essentials technical requirements must be flowed down the supply chain, and therefore a lead supplier would be expected to seek assurance that their sub-contractors are suitably compliant as well. The supply chain will also need to subsequently apply the same test as it flows work down into further sub-contracts, however it is recognised that the scoping statement may not be applicable at some of these lower levels.

Where the level of assurance required appears unclear then the upper standard should be applied. i.e. when there is uncertainty in the choice between Cyber Essentials and Cyber Essentials Plus then the requirements of the latter should be chosen as the default. For cyber risk levels above moderate it will be necessary to seek additional assurances above those offered by Cyber Essentials Plus.

There is no direct correlation between ISO27001 (Information Security Management) and the Cyber Essentials scheme; being certified to ISO27001 does not provide an equivalent level of assurance

unless the Cyber Essentials requirements have been included in the scope of ISO27001, and verified as such.

Selecting an appropriate level of assurance using the Cyber Essentials scheme based on the types of information:

	Cyber Essentials	Cyber Essentials Plus
Processing **any amount** of NDA OFFICIAL-SENSITIVE information on their own computer systems		YES
Processing some personal information on their own computer systems (relating to <100 people)	YES	
Processing **significant** volumes of personal information on their own computer systems on behalf of the NDA (relating to >=100 people)		YES
Processing some NDA OFFICIAL information on their own computer systems (relating to <50 records)	YES	
Processing **significant** volumes of NDA OFFICIAL information on their own computer systems (relating to >=50 records)		YES

Selecting an appropriate level of assurance using the Cyber Essentials scheme can also be based on the potential cyber risk level:

Cyber Risk Level	Criteria	Cyber Essentials
Insignificant	Contracts may be exempt where the 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 insignificant. In such cases it is suggested that a decision audit trail is recorded. E.g. There are certain contracts where there is no realistic cyber threat, for example communications/marketing planning services and certain facilities-related contracts.	N/a
Very Low	For contracts where a basic threat is faced (i.e. simple hacking, phishing or spyware) and where any attacker is likely to be opportunistic, unskilled and non-persistent. The sorts of contracts this will apply to are likely to be those covering commodity purchases or standard service provisions e.g. office supplies or the disposal of non-sensitive waste.	Cyber Essentials
Low	For contracts where the threat may be slightly more targeted (i.e. involving spear phishing, whaling or ransomware and where attackers are semi-skilled but may not be persistent). It is likely to apply to contracts for research or services but not where these are dealing with Sensitive Nuclear Information. This profile is likely to apply primarily to contracts handling information classified as OFFICIAL, but may also occasionally apply to those involving small quantities of OFFICIAL-SENSITIVE.	Cyber Essentials Plus
Moderate	For contracts subject to more advanced threats that are tailored and targeted with the objective of gaining access to specific assets or enacting denial of service. The attacker is likely to be persistent, organised and either be skilled or have access to skills e.g. cyber criminals or hacktivists. This will likely apply to contracts that involve handling greater volumes of, or more sensitive, personal information, and those involving larger quantities of OFFICIAL-SENSITIVE information. Contracts that involve the handling of Sensitive Nuclear Information are considered to be in this level.	Cyber Essentials Plus