What are the cyber threats?

The UK Cyber Security Strategy presented by the Cabinet Office describes in detail the threat (see section 2, pages 1 to 19). It identifies the top threats as criminals, state sponsored cyber actors, terrorists, and hacktivists.

The government's overarching vision

The government's vision is to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

What is the Defence Cyber Protection Partnership?

The Defence Cyber Protection Partnership (DCPP) is a joint industry and government response to the cyber security threat. The DCPP was established in 2013 by the Ministry of Defence (MOD), other government departments (OGDs), and defence suppliers working together to improve the cyber resilience of the sector in the face of increasing volume and sophistication of cyber attacks. Our vision is to work together to better understand the risk, improve the sharing of threat information, raise awareness and collaboratively develop a set of proportional measures to counter the threat that can be implemented via the contract.

The DCPP's primary output is the Cyber Security Model (CSM) which will apply to all new defence procurements form April 2017 (prime contracts only) and be fully implemented (with flowdown into supply chain) in October 2017. The CSM is a 3 stage process which assigns a level of risk to a contract, sets out the controls needed to mitigate that risk and assesses the supplier's ability to implement the risk mitigation measures. You can find further information about DCPP here.

What is the Cyber Essentials Scheme (CES)?

The CES is a set of measures that all organisations should implement to protect themselves against basic cyber threats on the internet. It was launched in June 2014. You can find further information about Cyber Essentials (CE), including how to apply for certification, at www.cyberstreetwise.com/cyberessentials/.

There are a number of different accreditation/certification bodies, how do I know which one to choose to gain Cyber Essentials certification?

We cannot make a recommendations of which accreditation body to use when obtaining Cyber Essentials. It is up to you to decide which body to use.

You can find information on the different accreditation bodies here. (https://www.cyberaware.gov.uk/cyberessentials/get.html)

Are there known scenarios where I may be unable to achieve Cyber Essentials certification?

You may be unable to achieve Cyber Essentials if any hardware or software on your network is unsupported by their manufacturer/developer and is deemed 'not supported'. This means that security updates cannot be developed and patched to these products.

If you are unable to achieve cyber essentials because of an MOD requirement you may be able to have this requirement waivered, this 'risk acceptance' process is outlined in DCPP CSM Industry Buyer and Supplier Guide. (URL to be determined)

How does MOD implement Cyber Essentials?

The Cabinet Office Procurement Policy Note (09/14) made it a mandatory requirement for suppliers performing certain types of government contracts to hold Cyber Essentials certification. MOD had previously made CES mandatory for all contracts from January 2016 prior to the implementation of its Cyber Security Model (CSM).

From April 3rd onwards all new contracts will include DEFCON 658 which sets out the requirements to hold Cyber Essentials or Cyber Essentials Plus.

Do I need Cyber Essentials Plus?

In line with MOD procurement policy note 09/14, Cyber Essentials Plus will be incorporated into the CSM, under which any contract assigned a risk level greater than 'Very Low' will require suppliers to hold Cyber Essentials Plus. Full details of the required cyber profiles are set out in DEFSTAN 05-138 available here.

Suppliers who expect to be bidding for such contracts in the future may wish to achieve the higher Cyber Essentials Plus level now.

How much does Cyber Essentials cost?

The cost of achieving Cyber Essentials certification through an official certifying body is approximately £300. This does not include the cost of any improvements required to achieve CE compliance. A Cyber Essentials certificate is valid for 12 months and must be renewed annually.

Companies applying for Cyber Essential for the first time may be eligible for a grant towards the cost. See Business finance support finder.

Further advice and information about free training is available here.

I am an overseas supplier – do I need to get Cyber Essentials before I can bid for UK MOD work?

Overseas suppliers may apply for and gain Cyber Essentials accreditation, this is not a UK only accreditation. International equivalents may also be acceptable. If you wish to offer an equivalent you should email issdes-dcpp@mod.uk at the earliest opportunity.

What is the Cyber Security Model (CSM)?

CSM means the process by which the authority ensures that its requirements to protect MOD Identifiable Information from cyber incident are implemented. The requirements are outlined in DEFSTAN 05-138. The CSM has 3 steps: a risk assessment is completed, a cyber risk profile is shared and a supplier assurance questionnaire is completed.

What is MOD identifiable information?

MOD Identifiable Information is any information held, processed or transferred electronically which is attributed to or could identify an existing or proposed MOD capability, and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure. Further information on what types of information would be classed as being included in or excluded from this definition can be found under 'Definition of MOD Identifiable' Industry Security Notice.

What is the Risk Assessment?

This is part of the Cyber Security Model and it is a short questionnaire which determines the cyber risk level for a contract or sub-contract. All Risk Assessments will be completed using the Supplier Cyber Protection Service.

What is the Supplier Assurance Questionnaire?

This is part of the Cyber Security Model and is used by the contractor to demonstrate compliance with the cyber protection requirements. All Supplier Assurance Questionnaires will be completed using the Supplier Cyber Protection Service.

What is Supplier Cyber Protection Service?

This is the online tool used to complete the Risk Assessment process and Supplier Assurance Questionnaire. You can view the specialist starting page for the Supplier Cyber Protection Service here.

At which point in the commercial process am I required to interact with the Supplier Cyber Protection service?

You will be informed of the Cyber Risk Profile through the contract notice that is published. To respond you will be required to register on the Supplier Cyber Protection Service and complete a Supplier Assurance Questionnaire as part of your tender submission. If it is a single source contract or there is no tender stage, you should submit the response by the date the contracting authority gives you.

Who should complete the Risk Assessment or Supplier Assurance Questionnaire?

The MOD does not require that any particular person or job holder complete a Risk Assessment or Supplier Assurance Questionnaire. We require that the person completing each questionnaire submit a declaration to say that you have the right to submit the response on your company's behalf.

Is there an annual requirement to review completed Risk Assessments or Supplier Assurance Questionnaires?

There will be an annual review of submitted Risk Assessments and Supplier Assurance questionnaires, this process will be handled by using the Supplier Cyber Protection Service.

How will I be notified when an annual review is due?

You will be notified using the Supplier Cyber Protection Service.

Do I have to flow down CSM requirements to my suppliers and subcontractors?

From October 2017 you must perform a Risk Assessment for each subcontract you place as part of delivering a MOD contract. You must inform your subcontractor of their responsibilities under DEFCON 658, this requires them to complete a Supplier Assurance Questionnaire and to complete a new Risk Assessment if they are sub-contracting any further. It is the always the responsibility of the contracting authority to ensure that its sub-contractor have in place the appropriate level of cyber protection measures for the Risk Level.

How will I know what cyber protection requirements will apply to my subcontract?

The contracting authority will identify the level of risk for the subcontract by completing a Risk Assessment on the Supplier Cyber Protection Service and the subcontractor will need to demonstrate that it has the required controls in place by completing a Supplier Assurance Questionnaire on the Supplier Cyber Protection Service. This will flow down through the supply chain as necessary (determined by the risk assessment).

I do not have Cyber Essentials or the appropriate risk mitigation measures. Can I still bid for the contract/subcontract?

As long as you can demonstrate you are working towards achieving Cyber Essentials or the appropriate risk mitigation measures and will have them in place prior to contract award you will be able to bid.

What happens if I will be unable to put the protection measures in place by the time of contract award?

MOD will, at its discretion, allow suppliers extended time to obtain the certification if they can prove it is due to delays in achieving certification and not due to a supplier failing the process. The supplier will be required to produce and implement a Cyber Implementation Plan.

What is a Cyber Implementation Plan (CIP)?

The CIP allows the supplier to set out the steps they commit to taking to achieve compliance together with a time frame for achievement. It should include detail on the current level of compliance, the planned measures to achieve compliance or the proposed mitigations for consideration. You can view the CIP template here.

What happens if I refuse to comply or implement the cyber protection measures?

Cyber protection measures are tender assessment criteria. You may be eliminated from the tender process as non-compliant if you do not comply with cyber protection requirements.

Will I be refused a contract if I am unable to achieve Cyber Essentials certification, or any other controls?

If you are unable to achieve compliance with any controls please contact your contracting authority who will be able to provide you with advice. There is a risk acceptance process outlined in the DCPP CSM Industry Buyer and Supplier Guide if you are unable to be compliant. If you are able to be compliant in the future but not by contract award date you will be able to submit a Cyber Implementation Plan.

Will cyber protection requirement be introduced retrospectively into extant contracts?

Cyber protection requirements may be introduced into extant contracts on a case-by-case basis. If they are, it will be via a contract amendment.

When tendering for contracts what are the cyber security control requirements?

The DCPP Supplier Assurance Questionnaire questions specify controls which are the minimum required for each risk level. The CSM on GOV.UK provides information on important considerations and best practice for each question. It is expected that companies will already have security measures in place to protect their businesses from cyber threats. Companies can enter a tender process without all controls in place, but they would be expected to have all the cyber protection measures necessary to fulfil the requirements of the contract in place at the time of contract award.

Do other government departments use the CSM in their procurements?

The CSM is currently only used by MOD but could be adopted by other government departments at some later date.

When will I have to be compliant?

Suppliers at all levels of the supply chain must have the cyber protection measures appropriate to the Risk Level in the contract/subcontract in place at the time of the contract/subcontract award.

How do I demonstrate compliance?

MOD requires a supplier assurance questionnaire to be completed on the Supplier Cyber Protection Service. MOD has the right to audit the responses submitted through this service to confirm they comply with the cyber protection requirements.

Where can I find the latest information about CSM requirements?

The DCCP webpage will be updated regularly with the latest information.

What are the existing cyber security controls and standards?

The Cyber Security Model (CSM) is based on well established controls from several existing standards. Most cyber security controls and standards are in place to address similar issues, therefore any existing investment in cyber security is likely to mean you are better prepared for CSM. We continue to work to align CSM with existing standards as much as possible and have mapped how many of them relate to the CSM and each other. This mapping will be published as we approach implementation.

What will be the impact on existing government requirements and guidance?

The Cyber Security Model is an additional requirement for doing business with MOD, while every effort has been made to reduce the amount of duplication for the time being the CSM does not replace any existing processes you must comply with.

What is the cost of implementing Cyber Essentials and CSM?

An important principle of the CSM is that it only specifies those controls which are necessary to mitigate the level of risk. This means companies only need to do what is necessary for the particular work with which they are involved.

Small businesses are as much a target for cyber attack as larger corporations, so it is equally important that they are protected.

It is important to note that the CSM specifies controls which are already considered good practice. Companies should already have appropriate security measures in place to protect their businesses, including from cyber threats.

Costs to companies

Cost to a company will depend on the company's cyber maturity and how well this is aligned to the risk they face. If your organisation already appreciates the cyber risk to its business and is implementing current industry best practices for cyber security then the Cyber Security Model (CSM) should have little effect beyond additional mapping to preferred standards and reporting requirements for assessment of compliance. If your organisation is not currently adopting best practice, or is unaware of the cyber risks it holds, the CSM will necessitate change within the organisation to meet the CSM requirements which, depending on the gaps identified, may require significant resources.

Grants towards achieving Cyber Essentials

DCPP's Cyber Security Model specifies controls which are already considered good cyber practice and are proportionate to the risk of the contract. It is expected that companies should already have appropriate security measures in place to protect their business, including from cyber threats. Where this is not the case then improvements will be at the company's own cost.

Various government initiatives may be available to support businesses to develop their cyber security and it may be possible to take advantage of these, companies can speak with trade associations. Companies applying for Cyber Essential for the first time may be eligible for a grant towards the cost. See Business finance support finder.

Responsibility for cyber security compliance

What happens if I am the victim of a successful cyber attack?

If a supplier has put in place all the cyber protection measures required by the contract is still the victim of a successful cyber attack MOD will not seek redress under the contract but will work with all involved to resolve the issue.

In accordance with DEFCON 658, the Supplier must report, as soon as they know or have reasonable grounds to believe, a Cyber Incident has occurred. The Supplier is to provide full details of the circumstances of the incident and any mitigation measures they have taken or intend to take. The buyer should consider each incident on a case-by-case basis and consult the Supplier before deciding on the appropriate action to take.

The DEFCON requires declaration of attempted cyber attacks – how quickly do MOD require declaration?

The MOD requires that you make a declaration as soon as you become aware that an attack/breach has been successful. We understand that on occasion this may be some time after the incident has occurred.

What is my liability in the event of a cyber breach?

Any party using the CSM process will only be in breach of the contract terms if they have failed to implement the cyber protection measures appropriate to the Risk Level of the contract/subcontract or made a false declaration when completing their Supplier Assurance Questionnaire.

Implementing the CSM requirements should increase a company's resilience, but no control regime guarantees full protection against all cyber attacks. Companies will be responsible for managing their own recovery from cyber incidents.

What are the benefits to a company in completing the Cyber Security Model?

The Cyber Security Model (CSM) will be a requirement of doing business with the MOD, but there are also additional benefits. For organisations who are less aware of the cyber threat, participating in the process can act as the first step in raising awareness of cyber security in their organisation. It will help to clarify what is expected and enable organisations to make targeted investments. It may also be used to highlight a company's capabilities to potential customers.

I have lots of contracts with MOD and its primes. Do I have to complete a Supplier Assessment Questionnaire for each contract?

All new contracts will require you to submit an SAQ response for each individual contract. If you are going to complete the work for different contracts within the same environment and on the same network you are able to copy and paste your answers from a previously completed SAQ. This should significantly reduce the amount of time needed to complete this process.

Will I become a preferred supplier if I complete a Supplier Assessment Questionnaire?

Completing the questionnaire will not make a company a preferred supplier.

Is compliance with the CSM mandatory?

The CSM will become an integrated element of the MOD's existing Acquisition System Guidance (ASG). It will be mandated at all stages of MOD acquisition, through contracts and supporting documents.

What is the cyber defence capability assessment tool (CDCAT)

CDCAT assessment and contract awards

The Cyber defence capability assessment tool is a cyber assessment approach developed by Dstl and now being marketed by the APM Group. It delivers a very thorough assessment of an organisations level of cyber protection and as such was considered too detailed to be used across the totality of the defence supply chain.

Whilst individual MOD contracts may specify compliance with CDCAT as a criteria for contract award this is not MOD policy. Once the CSM has been launched CDCAT will be one of a number of other assessment approaches that we will review to understand how it matches the controls set out in DEFSTAN 05/138 and if we are satisfied that it provides equivalent assurance we will allow suppliers who have successfully passed that to bypass some or all of the supplier assurance questionnaire.

What is the relationship between the CSM and Hadrian?

Hadrian questionnaire and the CSM supplier assurance questionnaire

The Hadrian questionnaire (sometimes also referred to as the Supplier information assurance tool (SIAT)) has been used in MOD for a number of years as our mechanism for assessing suppliers' information assurance. Its deployment has been based on campaigns run by individual TLBs and as such has reached only a small proportion of suppliers.

There is some overlap between the questions it asks and those in the Cyber Security Model 's supplier assurance questionnaire and so at the point when the CSM achieves equivalent penetration of the supply chain as Hadrian, then Hadrian will be withdrawn and the CSM will become the sole tool for supplier assurance. . This does mean that for a short period of time there may be a small number of suppliers who in quick succession are asked to complete both a Hadrian and CSM questionnaires but this will not endure.