

PROTECTING GOVERNMENT INFORMATION · GUIDE 4 OF 6

Cyber security

Cyber Essentials and the MOD Cyber Security Model, what each asks of a supplier and why the whole business is in scope.

WHERE THE REQUIREMENTS COME FROM

Two routes into the same systems

Cyber security protects the systems a business runs on, and with them every piece of government information those systems hold. Central government and the MOD set their requirements in different ways, and both reach well beyond the one folder where a contract's files are kept.

Source	What it asks for
Procurement Policy Note 014 Cyber Essentials scheme, February 2025	For central government contracts involving personal data or systems holding OFFICIAL information, Cyber Essentials, or Cyber Essentials Plus where the buyer judges the risk to be higher. A supplier without certification has to show equivalent controls.
Central government security schedule	The controls set out in the contract, recorded in your Security Management Plan, including any requirements for cloud services and remote access.
DEFCON 658 MOD contracts	Compliance with Defence Standard 05-138 at the level set for the contract, the Supplier Assurance Questionnaire every year, reporting of cyber incidents, and flow-down to subcontractors.
Defence Standard 05-138 Issue 4, May 2024	The controls themselves, graded by Cyber Risk Profile level. Mandatory for new and existing MOD procurements since 3 December 2025 under Industry Security Notice 2025/07.
Industry Security Notice 2024/06	Cloud services holding MOD information at OFFICIAL or OFFICIAL-SENSITIVE aligned with the National Cyber Security Centre Cloud Security Principles.

CENTRAL GOVERNMENT CONTRACTS

Cyber Essentials and the security schedule

Procurement Policy Note 014 applies to "all central government departments, their executive agencies and non-departmental public bodies, and NHS bodies". It sets when a supplier needs Cyber Essentials, and the security schedule in the contract sets the rest.

When Cyber Essentials is needed

The note applies to contracts involving citizens' personal data, government employee data, government business information or ICT systems that store or process OFFICIAL data. It also says plainly that "not all contracts will require suppliers to be certified", so the buyer decides, and chooses Cyber Essentials Plus where it judges the risk to be higher.

- **Timing.** "Evidence of holding a Cyber Essentials certificate (or equivalent) is essential at the point when data is to be passed to the supplier." The certificate is renewed every year.
- **Equivalence.** A supplier without the certificate can show equivalent controls, verified independently.
- **Third parties.** The note warns that Cyber Essentials does not bring a supplier's own providers, such as a cloud service, into scope. Check them separately.
- **Lapsed certificates.** A contract may exceptionally go ahead while a lapsed certificate is being renewed.

The security schedule

The Government Security Group publishes model security schedules on security.gov.uk, graded by the sensitivity of the data. Most ask the supplier to keep a Security Management Plan setting out its risk assessment and controls, and to review it every year. By default the schedules restrict remote working by privileged users unless the buyer approves a remote working policy.

Departments are themselves assessed against the National Cyber Security Centre Cyber Assessment Framework under GovAssure. A department may ask a supplier for evidence that supports its own assessment, so it helps to know which of your controls meet which of its outcomes.

MOD CONTRACTS

How the Cyber Security Model works

- 1 The MOD assesses the risk**
 The delivery team runs a risk assessment for the contract and gives it a Risk Assessment Reference and a Cyber Risk Profile level.
- 2 You answer the questionnaire**
 You complete the Supplier Assurance Questionnaire through the Supplier Cyber Protection Service. It is scored against the required level.
- 3 You close any gap with a plan**
 If you do not yet meet the level, you agree a Cyber Implementation Plan setting out what will be done and by when. It becomes part of the contract, and the dates in it need to be real.
- 4 You repeat it every year**
 The questionnaire is renewed on each anniversary of the contract, and records are kept for six years after the contract ends.
- 5 You flow it down**
 Equivalent provisions go into relevant subcontracts. As the prime, you assess the risk for each subcontract and pass the reference down.

The four levels

Level	Name	Controls	Cyber Essentials in Defence Standard 05-138
Level 0	Basic	3	Cyber Essentials
Level 1	Foundational	101	Cyber Essentials and Cyber Essentials Plus
Level 2	Advanced	139	Cyber Essentials and Cyber Essentials Plus
Level 3	Expert	144	Cyber Essentials and Cyber Essentials Plus

Control counts from clause 2.2 of Defence Standard 05-138 Issue 4. Controls 0001 and 0002 set the Cyber Essentials requirements. The level markings in the issue attached to your contract govern.

Version 4 of the model replaced the old profiles of Very Low, Low, Moderate and High. A document or contract still using those names is working from the previous model.

SCOPE

The whole business is in scope

For MOD work, Defence Standard 05-138 applies to "the Supplier's overarching corporate or enterprise environment", and Industry Security Notice 2026/01 confirmed in March 2026 that it applies to the supplier as a single legal entity. For central government work, the Cyber Essentials scope and the Security Management Plan need to cover every system that handles the contract's data.

A supplier that has carefully secured one project folder and left the rest of the business alone has misread the standard. Email, finance, the file server and the laptops used for other work are all part of the environment an attacker would come through. Cyber Essentials also works on a defined scope, and that scope needs to include wherever government information is actually handled.

What this means in practice

- **Plan to the highest requirement you hold.** A supplier with several contracts, whether MOD levels or central government schedules, will in practice run the business to the most demanding of them.
- **Keep the certificate scope honest.** A Cyber Essentials certificate that excludes the systems where contract work actually happens gives a customer a false picture.
- **Include your service providers.** Managed IT and cloud services are part of your environment. MOD flow-down reaches them, and central government buyers expect you to check them.
- **Look again when the business changes.** An acquisition or a new system can change what is in scope.

INDEPENDENT EVIDENCE

Cyber Essentials and Defence Cyber Certification

Cyber Essentials and Cyber Essentials Plus

The government-backed scheme covers five technical control themes: firewalls, secure configuration, security update management, user access control and malware protection. Cyber Essentials is a verified self-assessment. Cyber Essentials Plus adds hands-on technical testing. Both are renewed every twelve months, and the requirements were updated in April 2026 to version 3.3.

Defence Cyber Certification

Launched in May 2025 and run by IASME with the MOD, Defence Cyber Certification uses the same four levels as the Cyber Security Model. Under Industry Security Notice 2026/02, a valid certificate is accepted as assured evidence of compliance with Defence Standard 05-138 at that level, and a higher level covers the levels below it.

Two points to watch

The MOD Cyber Security Model guidance page still says certificate holders are not yet exempt from parts of the Supplier Assurance Questionnaire. Plan to complete both until the MOD confirms otherwise.

MOD has asked its industry partners to reach Level 0 by 31 December 2026, in Defence Digital publications in July and September 2026. It is a stated request, and no contract clause or notice sets it. Suppliers with a contract at a higher level already have that level to meet.

The Cyber Security and Resilience Bill, before Parliament in September 2026, would bring some managed service providers into regulation. It had not become law at the time of writing.

Incidents

For MOD work, cyber incidents are reported as DEFCON 658 requires and to the Defence Industry WARP, and a subcontractor also tells its prime. For central government work, follow the route in the security schedule.

EVIDENCE

What this area should produce

Record	What it shows
Cyber Essentials or Cyber Essentials Plus certificate, with its scope	Which parts of the business were tested, and when
Security Management Plan for each central government contract, with its annual review	The controls agreed with the buyer, and that they are kept current
Risk Assessment Reference and questionnaire result for each MOD contract	The level required and whether it was met
Cyber Implementation Plan and progress against it	That any gap is being closed on the agreed dates
Defence Cyber Certification certificate, where held	Assured evidence at a stated level
Cloud service review against the Cloud Security Principles	That services holding MOD information have been checked, at least yearly
Subcontract flow-down records	That cyber conditions reached the supply chain

Where this area meets the others

Cyber controls protect systems, and the people using them decide much of what happens to the information inside. A certified network does nothing about drawings forwarded to a personal account or printed at home, which is why Guide 5 treats information handling as its own area.

HOW THE MARK LOOKS AT THIS AREA

Under the Westmark Defence Supplier Mark, technical controls are examined in full at Cyber and Combined scope. Every assessment checks that contractual cyber obligations have been met. The Mark does not replace Cyber Essentials, Defence Cyber Certification or the Supplier Assurance Questionnaire, and a holder may not claim that it does.

WESTMARK ASSURANCE

Where the Defence Supplier Mark fits

Westmark Assurance provides independent security assurance, assessing organisations, premises and security arrangements against defined standards and frameworks.

The Westmark Defence Supplier Mark is for companies that supply defence and government. It assesses how an organisation identifies, controls and evidences security risk across the work it delivers, against a published standard and control set. The criteria are published in full at westmarkassurance.co.uk, so you can read exactly what is examined before you decide anything.

If you would like help putting these arrangements in place, we can introduce you to a Licensed Partner. Their preparation work is kept separate from our assessment, so an organisation they have supported is always assessed by someone independent of them.

Talk to us

For a conversation about the Defence Supplier Mark, or an introduction to a Licensed Partner:

hello@westmarkassurance.co.uk · 033 33 356 873

1st Floor, 2 West Regent Street, Glasgow, G2 1RW

Westmark Assurance is not an accredited certification body and does not offer UKAS-style certification. An outcome is a judgement by Westmark Assurance and carries no certification, accreditation or approval by government or the Ministry of Defence.

Westmark Assurance is a trading name of Ross Macdonald Consultancy Ltd, registered in Scotland, number SC848204. Registered office 1st Floor, 2 West Regent Street, Glasgow, G2 1RW.