

PROTECTING GOVERNMENT INFORMATION · GUIDE 1 OF 6

The protective envelope

How physical, personnel, cyber and information security combine to protect government information held by a supplier, and why each one can be done well while the whole still fails.

ABOUT THIS SERIES

Six guides for organisations that hold government information

If your organisation supplies a government department or the Ministry of Defence, some of the material you are given to work with will be marked OFFICIAL-SENSITIVE. Your customer expects it to be protected, and the contract usually says how.

These guides set out what that protection involves in practice. Each area of security can be put in place and evidenced on its own, and guides 2 to 5 treat them that way. Guide 6 shows how they join up, and how a supplier can show a customer that they do.

Guide 1	The protective envelope How physical, personnel, cyber and information security work together
Guide 2	Physical security Premises, storage, visitors and work on government sites
Guide 3	Personnel security Screening, vetting, briefing, aftercare and reporting culture
Guide 4	Cyber security The Cyber Security Model, Cyber Essentials and Defence Cyber Certification
Guide 5	Information security OFFICIAL-SENSITIVE handling and the devices that hold it
Guide 6	Bringing it together Evidencing one set of arrangements across all four areas

What OFFICIAL-SENSITIVE means

The Government Security Classifications Policy has three classifications: OFFICIAL, SECRET and TOP SECRET. OFFICIAL-SENSITIVE is a marking added to OFFICIAL information that is not intended for public release and is, in the policy's words, "of at least some interest to threat actors". Suppliers hold a great deal of it, which makes the supply chain one of the routes by which it can be reached.

Current at September 2026. Drawn from published UK Government and Ministry of Defence security requirements and National Cyber Security Centre guidance. Independent of government, and not produced or endorsed by any government department or the National Cyber Security Centre. Your contract and its security conditions take precedence over anything written here.

FOUR AREAS

Protective security is four areas that depend on each other

"Protective security comprises four interconnected domains, through which attacks are perpetrated: physical, personnel, cyber and technical."

Government Functional Standard GovS 007: Security, version 2.0, section 3.3

The government standard names technical security as its fourth domain. This series treats information security as the fourth area instead, because for a supplier most contractual obligations concern how information is marked, stored, sent and destroyed. Technical measures appear in guides 4 and 5 wherever they apply to a supplier.

Area	What it protects against	Where a supplier's obligations come from
Physical	Theft, loss, overlooking and unauthorised entry	The contract's security schedule or conditions, and the rules of each government site you visit
Personnel	People unsuitable for access, or whose circumstances change after they are given it	The Baseline Personnel Security Standard, and national security vetting where the contract needs it
Cyber	Attack on the systems the business runs on	Cyber Essentials under Procurement Policy Note 014, and for MOD work DEFCON 658 and Defence Standard 05-138
Information	Material reaching someone it should not, through the way it is marked, handled, sent or disposed of	The Classifications Policy, the contract's security schedule, and for MOD work the Security Aspects Letter and DEFCON 660

Someone trying to reach the information will use whichever route is easiest. Strength in one area does nothing for a weakness in another, which is why the government standard asks for security planning that is "holistic, covering all aspects". For a supplier, that means managing the four as one set of arrangements with one person accountable for them.

THE AUTHORITY CHAIN

How the requirements reach you

Government security policy binds departments, and the government standard expects each one to "set and communicate minimum contractual security requirements to suppliers". The route those requirements take differs between central government and the Ministry of Defence.

Central government contracts

The Classifications Policy applies to contractors handling government information in the same way it applies to civil servants. On top of it, a contract usually brings:

- **A security schedule in the contract.** The Government Security Group publishes model schedules on security.gov.uk, scaled to the sensitivity of the data from non-sensitive OFFICIAL through OFFICIAL-SENSITIVE, with a short form for lower-value work. Most ask the supplier to keep a Security Management Plan and review it every year.
- **Cyber Essentials.** Procurement Policy Note 014 requires it where a contract involves personal data or systems holding OFFICIAL information, with Cyber Essentials Plus where the buyer judges the risk to be higher.

Ministry of Defence contracts

- **Defence Conditions.** DEFCON 658 covers cyber security, DEFCON 660 covers OFFICIAL-SENSITIVE security requirements, DEFCON 659A applies to SECRET and above, and DEFCON 76 governs work at government establishments.
- **The Security Aspects Letter.** It says what is sensitive and attaches the OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions, currently Annex B to Industry Security Notice 2026/04. You return a signed acknowledgement before the work begins.
- **A Cyber Risk Profile** from Level 0 to Level 3, set under the MOD Cyber Security Model. You answer the Supplier Assurance Questionnaire against it every year of the contract.
- **Industry Security Notices**, published on gov.uk, which the conditions require you to follow. JSP 440, the MOD's own security manual, is not released to industry as a default.

Common to both. The requirements pass down to any subcontractor you use on the work, and you remain answerable for them. Both routes expect security incidents to be reported: to the contract manager under a central government contract, and to the Defence Industry WARP for MOD work.

WHERE THE GAPS SIT

When one area is covered and the next is not

The situations below are illustrations, written for this guide. In each one the organisation had one area of security properly in place, and the problem arose in an area nobody had looked at.

Situation	What was in place	What was not covered
A project laptop is encrypted and centrally managed. The engineer leaves it in a parked car overnight with the sign-in token in the same bag, and the car is broken into.	Cyber. The device met its configuration standard.	Physical and personnel. The conditions say devices are never left unattended in a vehicle and tokens are kept apart from them.
A screened and briefed designer forwards drawings to a personal email account to finish them at the weekend.	Personnel. Screening and briefing were done.	Information and cyber. Nothing prevented OFFICIAL-SENSITIVE material going to a personal account, which MOD conditions prohibit outright.
Paper copies are kept in a locked cabinet. A director prints a set at home to read on the train.	Physical. Office storage met the conditions.	Information. Home printing and reading in public took the material outside every control the company had.
A company holds Cyber Essentials Plus and has answered its Supplier Assurance Questionnaire. It sends the drawings to a survey subcontractor whose subcontract carries no security conditions.	Cyber. Its own systems were assured.	Supply chain. The conditions were never flowed down, so nobody set rules for the subcontractor.
An employee is approached online by someone asking about their work, and says nothing because they are worried about getting into trouble.	Personnel. The employee was properly screened.	Reporting culture. An approach the organisation should have heard about went unreported.

In every case the organisation could have produced a certificate or a record for the area it had in place. The problem arose where two areas met, somewhere nobody had been asked to look.

DOING IT IN PARTS

Each area can be evidenced separately

A supplier can build and evidence each area on its own, and many do.

Area	Evidence available	What it does not cover
Cyber	Cyber Essentials and Cyber Essentials Plus, for any government customer. For MOD work, Defence Cyber Certification at Levels 0 to 3 and the Supplier Assurance Questionnaire result.	How people handle information away from the systems, including through subcontractors.
Personnel	Baseline Personnel Security Standard checks, recorded by the employer. National security vetting, held by individuals through a sponsor.	Whether cleared people are briefed and report concerns, or whether the systems they use are secure.
Physical	Facility Security Clearance, for suppliers holding SECRET and above. Equipment rated in the NPSA Catalogue of Security Equipment.	Neither is required for OFFICIAL-SENSITIVE work, so most suppliers at that level hold no independent physical evidence.
Information	The supplier's own registers and records, the Security Management Plan under a central government schedule, and for MOD work the signed Security Aspects Letter acknowledgement.	No product, device or system is certified for OFFICIAL-SENSITIVE, and government guidance tells buyers not to look for one. The protection depends on how the organisation handles the information, which is what an assessment of its arrangements can examine.

Guides 2 to 5 each end with the evidence their area should produce. Each certificate is issued by someone looking at one area, and none of them examines whether the four fit together or who is accountable for the places where they meet.

LOOKING ACROSS ALL FOUR

The Westmark Defence Supplier Mark is an independent assessment designed to examine all four areas together, along with the governance, risk assessment, incident reporting and supply chain management that join them. Guide 6 explains how.

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.