The New Government Security Classification System -

A Guide for List X Defence Contractors

The guidance in this booklet is being developed for use from April 2014. It is not yet final but is being shared with industry in order to raise awareness on the New Government Security Classification policy.

If you have any questions on this document please email them to DBR-DefSy-STlndAH@mod.uk
Who should read this?

All personnel working for MOD contractors undertaking defence contracts on their own premises.
Everyone working for MOD contractors that handles information needs to understand this change.
Contractors performing work on MOD establishments work to separate security requirements as expressed by the establishment or local security officer and will have access to separate guidance.

Why this guide is important

From 2 April 2014 the Government is simplifying the way the UK classifies its information. This will involve new ways of working with information below SECRET level. All such information will now be classified OFFICIAL.

The introduction of OFFICIAL will take some getting used to, but the MOD strongly support the new approach to classification because it will help improve the way sensitive information is protected in the MOD and by defence contractors.

The key change is that individuals are expected to take more personal responsibility for thinking about the security of the information they handle.

This guidance is accompanied by additional industry communications providing more detailed information on managing the implementation of GSC.

It provides the basic guidance and tips for using the new system, including a one-page summary of the key points on page 2.

This guide is supported by:
- List X Notice 2014-01.
- An updated version of the Defence Security Handbook for MOD List X Contractors. (to be issued)

Version 0.1 14-02-2014

Government Security Classification System –
Key points on One Page

Why

- The change is being introduced on 2 April 2014 to enable a more flexible approach to security, while improving the security of government information by encouraging everyone to think more about how best to protect it.

What

- The old six classifications are reducing to three.
- Nothing is changing about dealing with information at the level of SECRET and TOP SECRET.
- The old classifications of CONFIDENTIAL, RESTRICTED, PROTECT and UNCLASSIFIED will no longer be used – except where this is specifically exceptionally necessary (for example to do business internationally or on certain contracts with industry e.g. Nuclear).
- From April 2014, all information below SECRET will automatically be classified OFFICIAL.
- Although there are important changes at the OFFICIAL level, none of these are particularly difficult.
- Information classified with the old markings does not need to be reclassified unless it is added to with new information – if not it should continue to be protected according to the previous rules.

How to Handle

- Unlike some other government departments, MOD policy is that MOD OFFICIAL information should not be routinely marked unless it is sensitive – in which case it should be marked (as you would expect) OFFICIAL-SENSITIVE; in some cases there may be a descriptor as well (see page 6).
- Unmarked MOD OFFICIAL information may be shared with recipients in the UK (including over the internet) provided you have no reason to think it needs greater protection or have been advised otherwise by the MOD (for example if it contains private personal data). So you just need to think whether you are aware of any sensitivity; this is a matter of common sense and the table on page 5 should help. MOD OFFICIAL information should not be released to the public without the prior approval of the MOD Contracting Authority.
- MOD OFFICIAL-SENSITIVE information should broadly be treated to the same standard as RESTRICTED information, with the important exception that subject to certain strict rules (pages 8 to 10) it can be sent unencrypted over the internet and even worked on using personal computers.
Why are these changes being made?

- So that the government genuinely has a single, shared approach to classification – it has not until now.
- To provide a simpler system – in today’s world we just don’t need six categories of classification.
- To improve information security by encouraging individuals to take more personal responsibility for the security of the information they handle, particularly at the OFFICIAL level.

Surely all this change and personal judgement/discretion increases the risk to sensitive information?

- No additional risk is being taken over the most sensitive information at SECRET and TOP SECRET.
- At the OFFICIAL level, any increased risk from relying on personal discretion will over time be offset by the new business flexibilities GSC enables, and also its focus on individual understanding and responsibility.

What does it all mean for people on the ground?

- This change will affect everyone in the MOD and defence contractors, but the impact on most people will not be great.
- The main changes are to do with:
  - the way we think about classifying and marking information – see pages 5 to 7; and
  - the way we share and transmit OFFICIAL information, particularly over the internet - see pages 8 to 10.
- In a few specific areas of business, for example where there is an international dimension or managing certain ‘legacy’ contracts at CONFIDENTIAL, some organisations will need to continue, at least for now, to work with the old classifications alongside the new. This is not ideal but is necessary to ensure that proper security is maintained with and by key partners outside UK government.
What will happen to information that was previously CONFIDENTIAL?

- Documents or assets classified CONFIDENTIAL under the old system that are not altered or added to do not need to be reclassified and should be protected exactly as before.

- Generally speaking, information that would previously have been classified CONFIDENTIAL will be tested by the MOD Contracting Authority to see if it meets the new criteria for SECRET (see page 6). If not, it will normally become OFFICIAL-SENSITIVE. Unless advised otherwise MOD contractors should continue to classify material according the latest version of the Security Aspects Letter (SAL) received from the MOD. MOD Contracting Authorities are having an action placed on them to review the security aspects of their contracts with industry and issue amendments to SALs in line with the normal contract amendment or SAL review point and, at the latest, by 1 April 2015.

- In a few specific areas of business, for example where there is an international dimension or managing certain ‘legacy’ contracts, there will be exemptions to allow continued use of CONFIDENTIAL - until further notice.

- For further guidance see List X Notice 2014-01 and Industry Security Notice 2014-01

Given the increased personal responsibility, what happens if there are breaches of security at OFFICIAL level?

- Within the MOD, individuals will be more personally accountable for information security under GSC.

- MOD looks to its Industry Partners to follow our principle of taking firm action if individuals:
  - have been careless or reckless with information they knew to be sensitive;
  - breach one of the clear mandatory rules (e.g. emailing MOD OFFICIAL-SENSITIVE information unencrypted across the internet without the approval of the originator); or
  - deliberately compromising the information (e.g. passing government information to a journalist without authorisation).
What makes information sensitive?

Information is sensitive if, in the wrong hands, it could potentially put at risk someone’s safety, or result in harm to the work of Defence or of the government more widely.

The table below illustrates the main kinds of ‘harm’ the MOD is concerned about, and where the ‘threat’ could come from.

<table>
<thead>
<tr>
<th>Potential Harm</th>
<th>Main Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place lives at risk.</td>
<td>Terrorists.</td>
</tr>
<tr>
<td></td>
<td>Foreign Intelligence Services/Hostile Forces.</td>
</tr>
<tr>
<td>Pose a threat to military, security or intelligence</td>
<td>Terrorists.</td>
</tr>
<tr>
<td>operations or operational capability.</td>
<td>Foreign Intelligence Services/Hostile Forces.</td>
</tr>
<tr>
<td></td>
<td>Criminals.</td>
</tr>
<tr>
<td></td>
<td>Campaign Groups intent on disrupting Defence activity.</td>
</tr>
<tr>
<td>Damaging UK stability or international relationships.</td>
<td>Foreign Intelligence Services.</td>
</tr>
<tr>
<td>Undermining the safe and effective conduct of military</td>
<td>Terrorists.</td>
</tr>
<tr>
<td>or MOD business.</td>
<td>Criminals.</td>
</tr>
<tr>
<td></td>
<td>Campaign Groups intent on disrupting Defence activity.</td>
</tr>
<tr>
<td>Damaging MOD’s commercial relationship with its suppliers.</td>
<td>Any individuals or groups prepared to exploit commercially sensitive information.</td>
</tr>
<tr>
<td>Serious Crime (including theft of Defence assets,</td>
<td>Terrorists.</td>
</tr>
<tr>
<td>information or money).</td>
<td>Criminals.</td>
</tr>
<tr>
<td>Threatening an individual’s privacy or vulnerability to</td>
<td>Criminals.</td>
</tr>
<tr>
<td>crime (e.g. by compromising personal data).</td>
<td>Especially cyber-criminals.</td>
</tr>
<tr>
<td>Undermining Ministerial Confidence by ‘leaking’</td>
<td>People working in Defence who are prepared to pass information to journalists, or otherwise make it public, without authorisation.</td>
</tr>
<tr>
<td>information to the media.</td>
<td></td>
</tr>
</tbody>
</table>
Some things that the MOD Contracting Authority will think about when classifying information

As advised previously, defence contractors will classify material according to the aspects defined in the latest version of the contract SAL issued by the MOD. The following provides some guidance on how the MOD may determine the appropriate classification:

1. In the wrong hands, could it pose a threat to life, or a serious risk to military, security or intelligence operations/capability, or to international relations? If so, it should be classified SECRET or TOP SECRET.

2. If information does not meet the tests for SECRET or TOP SECRET, then it is automatically classified as OFFICIAL.

3. Unlike some other departments, MOD policy is that OFFICIAL information should not be marked unless it is sensitive, in which case it should be marked OFFICIAL-SENSITIVE. In some cases a descriptor can be used following this marking. The only allowed descriptors are COMMERCIAL, LOCSEN (location sensitive) and PERSONAL.

4. Things that will be considered by the MOD in deciding whether to mark information OFFICIAL-SENSITIVE.

- If worried about the harm that could result from compromise to a foreign intelligence service or hostile forces, then it should probably be classified SECRET.

- What the potential harm is, and who poses the threat (see the table on page 5) is not about following some vague instinct. The information should be looked at on its own, and not how a foreign intelligence service, terrorist organisation, or other ‘threat actor’ could put it together with other information obtained from different sources. Classification should not be driven by arguments based on ‘what if everybody did this’.

- Consider if it were to come to light that the information had fallen into the wrong hands, would this lead to significant criticism of the MOD at the national level? If so, then a marking of OFFICIAL-SENSITIVE is probably right.

- Across the board, MOD would expect more than 80% of information to fall into the OFFICIAL category and therefore not be marked.
Government Security Classification (GSC) – Working with OFFICIAL Information

These are the main principles to be taken into account:

1. All information needs to be protected according to its sensitivity, but equally it can and should be shared (within the rules below) where this is sensible and helps deliver Defence business.

2. Use judgement and common sense in storing, working on and sharing information.

3. Think who the information might be at risk from, and protect accordingly.

4. Occasionally, you may have grounds to think information is sensitive even if it is unmarked (for example if it includes private personal information). If so, treat it as OFFICIAL-SENSITIVE and alert the originator to your concerns.

5. There are new flexibilities in sharing OFFICIAL information, which can be used if this helps deliver business more effectively.

Handling MOD OFFICIAL information

Unless you have reason to believe, or have been notified by the MOD Contracting Authority, that the content is sensitive (for example if it includes private personal information), documents or emails that have originated within the MOD and have no marking can be:

- emailed freely within the company.
- emailed unencrypted over the internet to third parties, provided you ensure that they understand any limitations that the MOD has determined needs to be applied to publication or further circulation of the information.
- discussed freely on all types of phone.
- physically taken and worked on at home and in public places.
- left unsecured when you leave your place of work, unless you judge this inappropriate (use common sense) or your business area has a ‘clear desk’ policy.
- disposed of in normal waste/recycling bins at work or at home.

If you are not sure whether the information is sensitive or not, you should treat as if it were OFFICIAL-SENSITIVE and seek advice from the MOD Contracting Authority or your local Security Officer.
Government Security Classification (GSC) – Working with OFFICIAL Information

Handling OFFICIAL-SENSITIVE information

Physical documents or emails with the OFFICIAL-SENSITIVE marking must be:

- locked in a secure container when not in use or you leave your place of work for more than half an hour.

- disposed of in a manner to make reconstruction unlikely, for example by shredding or burning.

They can be:

- emailed within the company and to the MOD across secure systems including the RLI and GSI.

- on an exceptional basis, emailed over the internet to third parties provided there is a business need, and subject to the prior approval of the MOD Contracting Authority (see page 9).

- physically taken and worked on at non-company locations but not read or worked on in public or otherwise in the sight of unauthorised people.

- discussed on all types of phone, but not with (or within earshot of) unauthorised persons.

- There are special rules for OFFICIAL-SENSITIVE information released to international partners and overseas contractors. Overseas, OFFICIAL-SENSITIVE will be handled to the standards applied to the recipients’ RESTRICTED information. The approval of the MOD Contracting Authority is required prior to its release. Where the release is a consequence of a sub-contract, the request for approval should be in accordance with the process described in the OFFICIAL-SENSITIVE Contract Security Condition. Further information can be found in List X Notice 2014-01 and Industry Security Notice 2014-01

Finally, if following the marking of OFFICIAL-SENSITIVE there is also a descriptor, the information must be stored electronically in locked down IT folders where access to it is limited to only those persons authorised to have such access.

Top Tips

- If you treat MOD OFFICIAL-SENSITIVE material as you used to treat RESTRICTED material you will avoid security breaches. But remember the two are not the same and there are new flexibilities you can use if this helps deliver your business.

- If in doubt about any aspect of handling MOD OFFICIAL information, protect it as if it were RESTRICTED and seek early guidance from your Security Officer or the MOD Contracting Authority.
Sending MOD OFFICIAL-SENSITIVE information unencrypted over the internet

- This will be permitted to recipients located in the UK, but only in exceptional circumstances. By definition, material with this marking needs careful protection and there is a risk that it could be compromised if transmitted unencrypted over the internet.

- However, internet transmission can be allowed provided there is a demonstrable and pressing business benefit, steps are taken to minimise the risk, and certain rules are followed:
  - there is no reasonable alternative and more secure means of achieving the business benefit.
  - the MOD Contracting Authority has given prior approval and when it is known that the intended recipient has been made aware of, and will comply with the requirements to protect MOD OFFICIAL-SENSITIVE information.
  - there is also appropriate company authorisation, normally by your Security Officer or line manager.
  - the covering email makes clear what the recipient can and can’t do with the information, and you must have confidence that this will be followed.
  - you must not send private personal information (in practice details going beyond standard information on a business card) without the person’s agreement.

**Top Tip: Think before you press send.** If the information you are about to email is compromised you will be asked to account for your actions and judgements and prove that you had the required approvals to send it this way. Are you sure you have identified the benefits, weighed the risks and followed the rules?
Government Security Classification (GSC) – Working with OFFICIAL Information

Working on MOD OFFICIAL information on personally owned computers

- One of the aims of GSC is to help people work more flexibly if they want to and if there is a business need.
- Some people may wish to work on MOD OFFICIAL information at home. Ideally this should be done on company issued and accredited Computer Information Systems but there will be times when this is not possible, and people may wish to work on MOD OFFICIAL information on personal computers or tablets.
- Under GSC, this will be allowed on an exceptional basis.
- The main rule is that this does not become ‘routine’; that there is always a clear business need, that produced or amended information is returned to the individual’s office within 5 days, and that the information and emails are deleted immediately thereafter, as fully as possible, from your personal machine (in case it is stolen or hacked).
- If the information is marked OFFICIAL-SENSITIVE, even tighter rules will apply. The main ones will be that:
  - there must be an exceptional compelling business need and the MOD Contracting Authority has given its prior approval in writing.
  - the user’s personal computer is compliant with the criteria in the MOD OFFICIAL - SENSITIVE Contract Security Condition.
  - the rules for emailing such material (see page 8 & 9) must be followed.
  - you must not process someone else’s personal information on your personal computer without their explicit permission.
  - Remember, if the information is compromised (e.g. if the device is stolen) you are accountable for how it was handled.

Working with ‘legacy’ information

- Information from before April 2014 with the markings PROTECT, RESTRICTED or CONFIDENTIAL should be protected under the old rules (which remain valid for this purpose).
- Existing information does not need to be reclassified unless it is amended or incorporated into new material.
- If circulating material with legacy markings, any covering paper/emails should be marked (or not) according to the new GSC system.
- Unmarked legacy material, or material marked UNCLASSIFIED should be treated as if it were OFFICIAL.
Government Security Classification (GSC) – Further Information

List X Notice 2014-01
Industry Security Notice 2014-01
Updated Defence Security Handbook For MOD List X Contractors

GSC on the GOV.UK website:
