

Government Security Classifications Policy

From Wikipedia, the free encyclopedia

The **Government Security Classifications Policy** (GSCP) is a new system for classifying sensitive government data in the United Kingdom.

Contents

- 1 GPMS
- 2 New classifications
 - 2.1 OFFICIAL
 - 2.1.1 OFFICIAL-SENSITIVE
 - 2.2 SECRET
 - 2.3 TOP SECRET
 - 2.4 Special handling instructions
 - 2.4.1 Descriptors
 - 2.4.2 Codewords
 - 2.4.3 Prefixes and national caveats
- 3 New approach to handling classified information
- 4 History
- 5 See also
- 6 References
- 7 External links

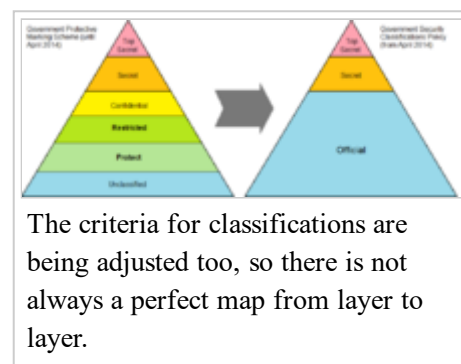
GPMS

Historically, the Government Protective Marking Scheme was used by government bodies in the UK; it divides data into UNCLASSIFIED, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. This system was designed for paper-based records; it is not easily adapted to modern government work and is not widely understood.^[1]

New classifications

The GSCP uses three levels of classification: OFFICIAL, SECRET and TOP SECRET.^[2] This is simpler than the old model and there is no direct relationship between the old and new classifications. "Unclassified" is deliberately omitted from the new model. Government bodies are not expected to automatically remark existing data, so there may be cases where organisations working under the new system still handle some data marked according to the old system.

Information Asset Owners continue to be responsible for information. The new policy does not specify particular IT security requirements - IT systems should be built and used in accordance with existing guidance from CESG.^[3]



Everybody who works with government - including contractors and suppliers - is responsible for protecting information they work with, regardless of whether it has a protective marking.

Aggregation does not automatically trigger an increase in protective marking. For instance, a database with thousands of records which are individually OFFICIAL should not be relabelled as a SECRET database. Instead, information owners are expected to make decisions about controls based on a risk assessment, and should consider what the aggregated information is, who needs to access it, and how.

OFFICIAL

OFFICIAL includes most public-sector data, including a wide range of information on day-to-day government business. It is not subject to any special risks. Personal data would usually be OFFICIAL.^[4] The data should be protected by controls based on commercial best practice instead of expensive, difficult specialist technology and bureaucracy. There is no requirement to mark every document as "OFFICIAL" - it is understood that this is the default for government documents.^[5]

Organisations may add "descriptors" to highlight particular types of official data, for instance commercially sensitive information about contracts, or diplomatic data which should not be seen by locally hired embassy staff. These descriptors do not automatically require special controls. "OFFICIAL" will usually include the kinds of data that were previously UNCLASSIFIED, RESTRICTED, or CONFIDENTIAL; but this may vary.

The threat model for OFFICIAL data is similar to typical large private-sector organisations; it anticipates that individual hackers, pressure groups, criminals, and investigative journalists might attempt to get information. The threat model does not guarantee protection against very persistent and skilled attacks, for instance by organised crime groups or by foreign governments; these are possible, but normal controls would make them more difficult, and much stronger controls would be disproportionate. People with routine access to OFFICIAL information should be subject to BPSS screening.

OFFICIAL may include data which is subject to separate regulatory requirements, such as the Data Protection Act (personal data) or PCI DSS (card payments).

OFFICIAL-SENSITIVE

OFFICIAL-SENSITIVE is an additional caveat for OFFICIAL data where it is particularly important to enforce need to know rules. OFFICIAL-SENSITIVE documents should be marked, but they are not necessarily tracked.

SECRET

"Very sensitive information", which might (for example) seriously harm national defense or crime investigations. Data should only be marked as SECRET if the SIRO agrees that it is high-impact *and* that the data must be protected against very capable attackers. Although some specialist technology might be used to protect the data, there is still strong emphasis on reuse of commercial security tools.

SECRET is a big step up from OFFICIAL; government bodies are warned against being overcautious and applying much stricter rules when OFFICIAL would be sufficient.

People with routine access to SECRET information should usually have SC clearance. SECRET data may often be exempt from FOIA disclosure.

TOP SECRET

Data with exceptionally high impact levels; compromise would have very serious impacts - for instance, many deaths. This requires an extremely high level of protection, and controls are expected to be similar to those used on existing "Top Secret" data, including CESG-approved products. Very little risk can be tolerated in TOP SECRET, although no activity is completely risk-free.^[6]

People with routine access to TOP SECRET information should usually have DV clearance. TOP SECRET information is assumed to be exempt from FOIA disclosure. Disclosure of such information is assumed to be above the threshold for Official Secrets Act prosecution.^[7]

Special handling instructions

Special handling instructions are additional markings which used in conjunction with a classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures. In addition to a paragraph near the start of the document special handling instructions include Descriptors, Codewords, Prefixes and national caveats.^[2]

Descriptors

A DESCRIPTOR is used with the security classification to identify certain categories of sensitive information and indicates the need for common sense precautions to limit access. The normal descriptors are 'COMMERCIAL', 'LOCSEN' and 'PERSONAL'.^[2]

Codewords

A Codeword is a single word expressed in CAPITAL letters that follows the security classification to providing security cover for a particular asset or event. They are usually only applied to SECRET and TOP SECRET assets.^[2]

Prefixes and national caveats

The UK prefix is added to the security classification of all assets sent to foreign governments or international organisations. This prefix designates the UK as the originating country and that the British Government should be consulted before any possible disclosure.^[2]

National caveats follow the security classification. Unless explicitly named, information bearing a national caveat is not sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals.^[2] Example

‘TOP SECRET – UK / US EYES ONLY’

With the exception of British Embassies and Diplomatic Missions or Service units or establishments, assets bearing the UK EYES ONLY national caveat are not sent overseas.^[2]

New approach to handling classified information

As before, the choice of classification is mostly based on the data's confidentiality requirements. Impact levels also consider integrity and availability, but CESG's system of Business Impact Levels (BIL) is under review, too.

The greater the consequences if the data were compromised, the higher the classification. Information systems will continue to be accredited much as before, normally using CESG Information Assurance Standard 1 & 2. Storage media which hold UK government data should still be destroyed or purged according to HMG IA Policy No. 5.

Higher classifications require stricter personnel vetting.

History

The Government Security Classifications Policy was completed and published in December 2012; additional guidance and supporting processes were developed over time.

Government bodies (and the armed forces) were expected to start using the GSCP in April 2014.

See also

- Security Policy Framework
- Information Assurance Standard 1 & 2
- Cabinet Office
- List X site
- Compartmentalization (information security)
- Security vetting in the United Kingdom

References

1. An Introduction to Government Security Classifications. Page 1. Cabinet Office, April 2013
2. *Government Security Classifications* (PDF) (Version 1.0 – October 2013 ed.). HMG Cabinet Office. April 2014. Retrieved September 10, 2014.
3. Government Security Classifications FAQ Sheet 2: Managing Information Risk at OFFICIAL. Cabinet Office, April 2013
4. An Introduction to Government Security Classifications, Cabinet Office, April 2013
5. Government Security Classifications FAQ Sheet 1: Working with OFFICIAL Information. Cabinet Office, April 2013
6. Government Security Classifications: Security Controls Framework. Cabinet Office, April 2013
7. Government Security Classifications: Security Controls Framework, page 19. Cabinet Office, April 2013

External links

- Government Security Classifications on the Cabinet Office website (<https://www.gov.uk/government/publications/government-security-classifications>)
- Government Security Classifications video (https://www.youtube.com/watch?v=_s9AuJdei64)
- Ministry of Defence Industry Security Notice 2014/1 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/282902/isn_2014_01_gov_security_class_scheme.pdf)
- PSN Community Briefing (<https://www.publicservicesnetwork.service.gov.uk/article/2074/PSN-publishes-community-briefing-on-new-Government-Security-Classification-Policy>)
- Cybermatters blog post on the scheme (<http://cybermatters.info/2014/04/01/uk-government-security-classification-scheme/>)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Government_Security_Classifications_Policy&oldid=696416548"

Categories: [Classified information](#) | [Privacy](#) | [Government of the United Kingdom](#) | [Information sensitivity](#)
| [Public policy in the United Kingdom](#)

- This page was last modified on 23 December 2015, at 00:25.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.