Whitepaper on the Government Classification Scheme (by Nigel Strutt)

Introduction

Irrespective of the views of parties across Government, suppliers and the security communities the new Government Classification scheme is going 'live' in April 2014, with the Police sector following in October 2014.

This paper is intended to provide some guidance on HOW the classification scheme could work, and in particular the impact on current working arrangements and interfaces to systems/networks at a local and national level that do not recognise the classification scheme.

Throughout the document reference is made to statements made by Cabinets Office concerning issues associated with the Government Classification scheme. The author's response to each issue is also provided ('boxed').

Background

Useful reference material can be found on the Cabinet Office web site can be found at:

- https://www.gov.uk/government/publications/government-security-classifications
- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf

Including:

- Working with OFFICIAL information
- Government Security Classifications April 2014
- Managing information risk at OFFICIAL
- Working with personal information

Mapping from 'Old' to 'New'

Not Protectively Marked

"The new classification system has quite purposefully taken UNCLASSIFIED (or 'Not Protectively Marked') out of the equation. ALL information that is created, collected, processed, stored or shared within government (and across the wider Public Sector) has value, belongs to the organisation and must be handled with due care."

'Not Protectively Marked' does not exist as a protective marking and all information will be OFFICIAL as a minimum.

RESTRICTED and CONFIDENTIAL

"There is no direct correlation between the new classification policy and the old GPMS scheme. In general terms, assets that were previously classified up to and including RESTRICTED should be managed at OFFICIAL. Although the review found instances where some information was over marked at CONFIDENTIAL and this may be appropriate to manage as OFFICIAL too. Originators need to think about the nature and context of any information they handle when deciding whether it is appropriate to particularly enforce need to know through use of the OFFICIAL-SENSITIVE caveat."

"There is a materially different threshold for SECRET assets, both in terms of threat and the impact of compromise. RESTRICTED (or CONFIDENTIAL) information should only move into the SECRET tier if the organisation's SIRO has assured themselves that BOTH the consequences of compromise or loss correspond to the impact statements set out in the classification policy; AND that the information needs to be defended against highly capable, determined and well-resourced threat actors as described in the SECRET threat profile (in essence hostile foreign intelligence services or high-end organised crime groups)."

> It is the author's opinion that data which would have been marked as RESTRICTED should be marked OFFICIAL-SENSITIVE, whilst data which would have been marked as CONFIDENTIAL should also be marked as OFFICIAL-sensitive. At this point what becomes important is the protection which is mandated for OFFICIAL-SENSITIVE.

Aggregation

"Aggregation of large amounts of personal data has no bearing on the application of classification markings, but it can change the threat to the information and also enhance the impact of any compromise. Where large data sets of personal information exist in the OFFICIAL classification, effective procedural, and in some cases technical, controls may be appropriate to reinforce the „need to know" principle and provide enhanced protection. However the data should not be marked OFFICIAL-SENSITIVE."

> It is clear that aggregation does not change the protective marking of the application / system but may affect the level of threat.

Integrity and Availability

> No further advice has been given by Cabinet Office on the proposed changes to the marking scheme with regard to Integrity and Availability. Hence the author recommends that the current marking scheme based on Impact levels continue to be used.

Threat model

"The Threat Profile for OFFICIAL does not include highly capable, determined and well resourced organised crime groups and state actors."

> The effect of this statement is to reduce the potential risks to the assets that are marked as OFFICIAL because the IS 1 assessment will only consider threat sources and actors ('external' threat) with a 'lower' level of capability

Marking assets

Blank

"There is no requirement to mark routine OFFICIAL information."

> The author recommends that all information is marked eith OFFICIAL, OFFICIAL-SENSITIVE or SECRET.

OFFICIAL-SENSITIVE

"Organisations and staff should use their discretion to determine those instances where it will be appropriate to use the OFFICIAL-SENSITIVE caveat as this will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements. Organisations need to make their own judgements about the value and sensitivity of the information that they manage, in line with departmental and HMG corporate risk appetite decisions.
However, the handling caveat should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for HMG more generally. This might include, but is not limited to the following types of information:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to ministers on contentious and very sensitive issues;
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- more sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but does not require SECRET-level protections;
- diplomatic activities or negotiating positions where inappropriate access could impact foreign relations or negotiating positions and must be limited to bounded groups;
- very sensitive personal data

Descriptors

"Three optional descriptors may be used (in conjunction with a security classification) to distinguish specific types of information in the following circumstances"

- To limit circulation of sensitive information that locally engaged staff overseas cannot access
- To distinguish commercial or market sensitive data, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed
- To identify particularly sensitive information relating to an individual (or group), where inappropriate access could have damaging consequences"

> There doesn't appear to be guidance on the format of the descriptors. Organisations should use the descriptors commonly used today, e.g. COMMERCIAL, PERSONNEL / PRIVATE, UK STAFF ONLY

OFFICIAL vs SECRET

Organisations must be mindful that there is a very significant step-up (a cliff face) from OFFICIAL to SECRET, and that the benefits of the new policy will be eroded if they are too risk averse and seek to put more information into SECRET then is absolutely necessary.

> The requirements for controls pertaining to information assets marked as SECRET remain unchanged; see existing IA Standards and GPGs for details.

Who can mark / unmark a document?

"The originator is responsible for determining the appropriate classification for any assets they create, though recipients / holders of copies may challenge the classification with a reasoned argument if necessary. Depending on context and circumstances sensitivities may change over time and it may become appropriate to reclassify an asset.
Every effort should be made to consult the originator or originating organisation before a sensitive asset is considered for disclosure, including release under FOIA or to the National Archives."

> Requirements pertaining to the ownership of an information assets, and in particular the responsibility for choosing a marking resides with the originator.

Does existing information need to be remarked?

"Organisations are not required to retrospectively remark legacy information or data that uses the old protective markings. Furthermore information or data does not need to be remarked where it is in continued use within an organisation, provided that users / recipients understand how it is to be handled in line with the new Classification Policy. However, where legacy information or data bearing a former protective marking is to be shared or exchanged between organisations, or with external partners, the originator should consider remarking with the appropriate security classification. At the very least, meaningful guidance should be provided about how the asset should be protected in line with the new approach. "

> No need to retrospectively remark legacy information, however where legacy information or data bearing a former protective marking is to be shared or exchanged between organisations, or with external partners, the originator should consider remarking with the appropriate security classification.
>
> Wherever practical the 'new' classification scheme should be used – and that may mean 'double' markings existing information assets with the 'old' and 'new' markings.

Impact levels

"There is no longer any mandatory or policy requirement for the use of BILs and they do not map to the new classifications"

> The author recommends that the Impact levels defined in Infosec Standard No. 1 continue to be used to classify a system.

Data Protection Act

"The DPA requirement to provide appropriate and proportionate protection for personal data is unchanged. Senior Information Risk Owners (SIROs) and IAOs need to assure themselves that they have taken reasonable steps to comply with the DPA principles."

> The DPA requirement to provide appropriate and proportionate protection for personal data is unchanged.

Level of protection

> There have been no changes (as yet) to the Infosec Standards and Good Practice Guides -and as such the 'old' versions remain valid.

OFFICIAL

"Personnel, physical and information security controls for OFFICIAL are based on commercial good practice, with an emphasis on staff to respect the confidentiality of all information."

> Good commercial practice includes the following technical requirements:
>
> a. Strong authentication
> b. Protection for 'data at rest' (and ideally not residing on the 'local device
> c. Protection for 'data in transit'
> d. Access control (with regard to business information and applications)
> e. Anti-virus
> f. Regular patching
> g. Corporate control over the use of administration rights
> h. Firewall (and IPS)
> i. Asset registers
> j Event logging for accountability purposes
> k. Security review and testing
>
> Implementation of these requirements may be undertaken using 'main stream' commercial security products.

OFFICIAL-SENSITIVE

> It is the author's opinion that the controls which protect OFFICIAL-SENSITIVE compared to OFFICIAL are:
>
> a. 'Stronger'. Note the actual types of controls used to implement the requirement could be different, e.g. smartcard-based authentication as opposed password
> b More assurance that the controls are working properly
> c Additional (or enhancements to the) requirements for controls, e.g. Intrusion detection
> d Enforced by a governance regime that is 'pro-active, well-managed, resourced by professionals
> e Documented in a Risk Management & Accreditation Document Set (RMADS), which also includes a risk assessment, statement of the requirements for controls (and their implementation status) and Operating procedures

SECRET

No change to the Infosec Standards, Good Practice Guides as they relate to the protection of SECRET assets.