CESG

The Information Security Arm of GCHQ

Making Sense of the new Government Security Classifications Policy

(The Who, What, When and Why)

Geoff Eden
Deputy Technical Director
Public Sector Services

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP

The Who…

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The Who

- First and foremost – this is not a CESG policy
- It is sponsored by the Minister for the Cabinet Office

- and forms part of the Civil Service Reform Plan
- Though you do have to look quite hard…

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The Who

- Page 29, a bullet under 'Modernising Security across the Civil Service' – 'Simplify Security Classifications'
- The Government Security Secretariat (GSS) was subsequently tasked to create the new GSCP
- So if I haven't mentioned already ☺ this is not a CESG policy – though we have supported its development

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP

The What…

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- Simplification will take the form of a rationalisation of the current six tier model into three ‘distinct and intuitive’ security domains…
- Currently we have six tiers under the existing protective marking system (the GPMS): UNCLASSIFIED, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET which will be replaced with

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

TOP SECRET

HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- There is no requirement to mark routine OFFICIAL information
- There will be a limited subset of OFFICIAL information which could have more damaging consequences should it be compromised
- This will be marked OFFICIAL-SENSITIVE and could have an optional DESCRIPTOR
- Greater 'need to know' assurances are required (generally through procedure and/or personnel)

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- This does not introduce another tier within OFFICIAL!
- I am (sadly) privy to a lot of this:
  - UNCLASSIFIED OR PROTECT = OFFICIAL
  - RESTRICTED = OFFICIAL-SENSITIVE
- Or
  - IL0 OR IL1 OR IL2 = OFFICIAL
  - IL3 = OFFICIAL-SENSITIVE

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- As well as the usual impact of compromise statements that we have in the current protective marking system the GSCP introduces applicable threat profiles for each security domain
- This is very useful and helps to moderate risk management thinking – we cannot possibly expect to protect all HMG assets from every single threat!

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- Threat profiles should be viewed from the perspective of capability
- We talk about a commercial threat model for OFFICIAL - a threat profile broadly similar to that faced by a large UK private company
- The threat profile for SECRET anticipates the need to defend against a higher level of capability

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- The threat profile for TOP SECRET reflects the highest level of capability deployed against the nation's most sensitive information and services
- So for example, where we have very sensitive information, which should it be compromised, directly threatens an individual's life **AND** requires protection against a highly capable threat it will be SECRET

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- Asset owners should think about how they mark their assets under the new GSCP, (and the supporting risk management processes), not map
  - UNCLASSIFIED OR PROTECT = OFFICIAL
  - RESTRICTED = OFFICIAL-SENSITIVE
- Or
  - IL0 OR IL1 OR IL2 = OFFICIAL
  - IL3 = OFFICIAL-SENSITIVE

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- The main policy document is supported by an annex – Security Controls Framework and a series of FAQs
- It is very much a policy document not a standard which is split into three sections:
  - Part One – Threat Model and Security Outcomes
  - Part Two – Working with HMG Assets
  - Part Three – Protecting Assets and Infrastructure

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The What

- In a nutshell it presents more assurance and more senior oversight as we work with higher security classifications
- So what about CESG's IA policy and guidance?
- It remains extant as many of these documents describe good practice which is agnostic of security classifications

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP

The When…

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The When

- The policy has been complete for some time (version 1.0 December last year) with the supporting annex completed in April of this year
- There are some FAQs which are yet to be completed
- The new policy is possibly the worst kept secret in government…
- There are plenty of websites which already mention the new policy

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The When

- So I understand that there will be both an internal and external launch soon
- The launch will initiate a six month countdown for government until the go-live date of **2 April 2014**
- This allows Departments to launch their own local training and communications activity and begin briefing and preparing their staff for the new ways of working

CESG

The Information Security Arm of GCHQ

Making Sense of the new GSCP

The Why…

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The Why

- Cabinet Office will often be heard saying things like this:
  - It will improve efficiency
  - It will be more intuitive
  - Current arrangements are unwieldy
  - It will save money? Certainly in the longer term

CESG
The Information Security Arm of GCHQ

Making Sense of the new GSCP – The Why

- However, the why that's emerging for me is that this is acting as a catalyst for more effective risk management
- By that I mean traceable security which supports the business
- Organisations are starting to look at their risk management processes under the existing protective marking system and question their applicability and effectiveness – this can only be a good thing!

CESG

The Information Security Arm of GCHQ

Making Sense of the new GSCP