Cabinet Office

Government Security Classifications

May 2018

Version 1.1 – May 2018

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
11.0	1.0	Oct 13	N/A – This document will replace the current 'Government Protective Marking Scheme' document on 2 April 2014.
SPF Version	**Document Version**	**Date Published**	**Summary Of Changes**
11.0	1.1	May 18	This document will replace Document Version 1.0 for the purpose of making reference to Data Protection legislation as outlined as follows: • Overview of Key Principles, paragraph 1, page 4 • Official - Definition, page 7 • Disclosure, page 27 Including referencing the exemptions to some or all of the data protection principles as outlined as follows: • Legal Framework, paragraph b, page 15 The EU-US Privacy Shield replaces the Safe Harbor Agreement, which was held to be invalid in October 2015 by the Court of Justice of the European Union. These changes have been reflected at the Annex, under Part Three, Technical Controls Summary, paragraph 53.

Government Security Classifications

Executive Summary

This policy describes how HM Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

Everyone who works with government has a duty to respect the confidentiality and integrity of any HMG information and data that they access, and is personally accountable for safeguarding assets in line with this policy.

HMG information assets may be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

Government Departments and Agencies should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. NDPBs and Arms Length Bodies) and wider supply chain.

The Government Security Classifications will come into force on 2 April 2014 – until then existing policy remains extant.

Cabinet Office
December 2012

Government Security Classifications

December 2012

Overview of Key Principles

1. This policy describes HM Government's administrative system for the secure, timely and efficient sharing of information. It is not a statutory scheme but operates within the framework of domestic law, including the requirements of the Official Secrets Acts (1911 and 1989), the Freedom of Information Act (2000) and Data Protection legislation.

Principle One:
ALL information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

2. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification:

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.

3. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. A top level controls framework is provided as an annex to this policy. As a minimum, all HMG information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. There is no requirement to mark routine OFFICIAL information.

4. Organisations may need to apply controls above (or below) the baseline on a risk managed basis appropriate to local circumstances and in line with HMG risk appetite tolerances. The Government SIRO will moderate such instances that entail any pan-government risk.

5. The classification scheme applies to information (or other specific assets). Major ICT infrastructure (e.g. large aggregated data sets, payments systems, etc.) may require enhanced controls to effectively manage associated confidentiality, integrity and availability risks – determined on a case by case basis following a robust risk assessment.

Principle Two:
EVERYONE who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

6. Accidental or deliberate compromise, loss or misuse of HMG information may lead to damage and can constitute a criminal offence. Individuals are personally responsible for protecting any HMG information or other assets in their care, and must be provided with guidance about security requirements and how legislation relates to their role, including the potential sanctions (criminal or disciplinary) that may result from inappropriate behaviours. A summary of the relevant legal and regulatory context is set out on page 13.

7. Organisations must have a breach management system in place to aid the detection and reporting of inappropriate behaviours, enable disciplinary procedures to be enforced and assist with any criminal proceedings.

Principle Three:
Access to **sensitive** information must **ONLY** be granted on the basis of a genuine 'need to know' and an appropriate personnel security control.

8. Information needs to be trusted and available to the right people at the right time. The failure to share and exploit information can impede effective government business and can have severe consequences (e.g. medical records or case management files). The principles of openness, transparency, Open Data and information reuse require individuals to consider the proactive publishing of public sector information and data sets. However, this must always be a reasoned judgement, taking data protection and confidentiality into account.

9. The compromise, loss or misuse of sensitive information may have a significant impact on an individual, an organisation, or on government business more generally. Access to sensitive information must be no wider than necessary for the efficient conduct of an organisation's business and limited to those with a business need and the appropriate personnel security control. This 'need to know' principle applies wherever sensitive information is collected, stored, processed or shared within government and when dealing with external public and private sector organisations, and international partners.

10. The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements. In extremis, there may be a need to share sensitive material to those without the necessary personnel security control, for example when immediate action is required to protect life or to stop a serious crime. In such circumstances a **common sense** approach should be adopted - if time permits, alternatives should be considered and steps taken to protect the source of information. If

there is any doubt about providing access to sensitive assets, individuals should consult their managers or security staff before doing so and when time permits record the reasons for their actions.

Principle Four:
Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

11. The policy applies equally to assets entrusted to HMG by others, such as foreign governments, international organisations, NGOs and private individuals.

12. Where specific reciprocal security agreements / arrangements are in place with foreign governments or international organisations, equivalent protections and markings must be recognised and any information received must be handled with AT LEAST the same degree of protection as if it were UK information of equivalent classification. Detailed information about international and bilateral security agreements and the controls for managing foreign-originated information is set out in the 'International Protective Security Policy' supplement to the SPF.

13. Where no relevant security agreements / arrangements are in place, information or other assets received from a foreign country, international organisation or a UK NGO must at a minimum be protected to an equivalent standard as that afforded to HMG OFFICIAL assets, although higher classifications may be appropriate. Refer to the 'International Protective Security Policy' supplement for more detail.

14. The need to know principle must be strictly enforced for access to international partners' information.

Security Classification Definitions

15. The three security classifications (OFFICIAL, SECRET and TOP SECRET) indicate the increasing sensitivity of information AND the baseline personnel, physical and information security controls necessary to defend against a broad profile of applicable threats:

- The typical threat profile for the **OFFICIAL** classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.
- The threat profile for **SECRET** anticipates the need to defend against a higher level of capability than would be typical for the OFFICIAL level. This includes sophisticated, well resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors. Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks.
- The threat profile for **TOP SECRET** reflects the highest level of capability deployed against the nation's most sensitive information and services. It is assumed that advanced state actors will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.

OFFICIAL

Definition:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile described in paragraph 15 above, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under Data Protection legislation or other legislation (e.g. health records).

Baseline Security Outcomes:

- **ALL** HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice (described in the Annex).

Marking:

There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

16. Data Owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate.

17. To support specific business requirements and compartmentalise information, organisations may apply an optional DESCRIPTOR, alongside the OFFICIAL-SENSITIVE classification marking, to distinguish particular types of information and indicate the need for additional common sense precautions to limit access. Further detail is provided in paragraph 21 below.

SECRET

Definition:

Very sensitive HMG (or partner's) information that requires protection against the highly capable threat profile described in paragraph 15, **AND** where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Directly threaten an individual's life, liberty or safety (from highly capable threat actors).

b. Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:

   i. Current or future capability would be rendered unusable;

   ii. Lives would be lost; or,

iii. Damage would be caused to installations rendering them unusable.

c. Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.

d. Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.

e. Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.

f. Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.

g. Cause major impairment to the ability to investigate or prosecute serious organised crime.

Baseline Security Outcomes:

- Make accidental compromise or damage highly unlikely during storage, handling, use, processing, transmission, transport or disposal.
- Offer an appropriate level of resistance to deliberate compromise by forced and surreptitious attack.
- Where possible, detect actual or attempted compromise and help to identify those responsible.

Marking:

All information in this security domain should be clearly and conspicuously marked **'SECRET'**. Information that requires more restrictive handling due to the nature or source of its content may merit a special handling instruction; see paragraphs 18 – 26 below.

TOP SECRET

Definition:

Exceptionally sensitive HMG (or partner's) information assets that directly support (or threaten) the national security of the UK or allies **AND** require extremely high assurance of protection from all threats (as set out in paragraph 15). This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Lead directly to widespread loss of life.

b. Threaten directly the internal stability of the UK or friendly nations.

c. Raise international tension.

d. Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.

e. Cause exceptionally grave damage to relations with friendly nations.

f. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

g. Cause long term damage to the UK economy.

h. Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

Baseline Security Outcomes:

- Prevent accidental or deliberate compromise or damage during storage, handling, use, processing, transmission, transport or disposal.
- Offer robust resistance against compromise by a sustained and sophisticated or violent attack.
- Detect actual or attempted compromise and make it likely that those responsible will be identified.

Very little information risk to such data and services can be tolerated unless there is full and explicit understanding by the SIRO in line with HMG risk appetite tolerances.

Marking:

All such information should be clearly and conspicuously marked **'TOP SECRET'.** Information that requires more restrictive handling due to the nature or source of its content may merit a special handling instruction; see paragraphs 18 – 26 below.

Special Handling Instructions

18. Security classifications are the principle means of indicating the sensitivity of a particular asset and the requirements for its protection. Special handling instructions are additional markings which can be 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.

19. Special handling instructions should be used sparingly and only where the sensitivity justifies strict restrictions on information sharing. Individuals must be given guidance on how to mark and work with assets bearing special handling instructions.

20. A supplementary control framework for handling material derived from intelligence is provided in the SPF.

DESCRIPTORS

21. Organisations may apply a DESCRIPTOR to identify certain categories of **sensitive** information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: '**OFFICIAL-SENSITIVE [DESCRIPTOR]'**

22. Cabinet Office maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments:

    - **'COMMERCIAL':** 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.
    - **'LOCSEN':** Sensitive information that locally engaged staff overseas cannot access.
    - **'PERSONAL':** Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records of people in sensitive posts (e.g. military, SIA).

23. Descriptors must not be applied to information that is sent to overseas partners (unless formally agreed in advance) as they are not recognised under any international agreements and are likely to cause confusion.

CODEWORDS

24. Codewords provide security cover for a particular asset or event. A Codeword is a single word expressed in CAPITAL letters and is placed immediately after the classification marking. They are usually only applied to SECRET and TOP SECRET assets. Codewords are co-ordinated centrally by the Defence Crisis Management Centre and must be allocated by the centre's Operational Support team.

PREFIXES AND NATIONAL CAVEATS

25. Specific markings may be used either to indicate the provenance of sensitive information, or as a means to control dissemination.

    a. UK Prefix - ALL assets sent to foreign governments or international organisations, must be marked with a UK prefix, both to designate the originator and to inform any decision about possible disclosure under existing or future Freedom of Information (FOI) legislation in the country concerned. SECRET and TOP SECRET assets should include the following instruction:

    b. National Caveats may be used to designate assets of particular sensitivity to the UK or where dissemination must be restricted to individuals from specific foreign nations. Unless explicitly named, information bearing a national caveat must not be sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals (either overseas or in the UK) without the originator's consent. Information should be marked in the format 'CLASSIFICATION – CAVEAT', e.g:

'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 must only be sent overseas in exceptional circumstances and where access by British nationals can be strictly controlled.

Time Sensitive Information

26. In carefully controlled circumstances, it may be appropriate for some high-value, high-threat information to be managed at a lower classification to capitalise on immediate business and/or operational benefits, for example where the value of the information is time limited and short term. Such 'one off' exceptions must be carefully considered and the organisation's Senior Information Risk Owner (SIRO) must fully understand the longer term risk implications for their business given that an adversary may invest to discover vulnerabilities now that can be very quickly capitalised on in the future. This is particularly important if the same capabilities are used frequently or over an extended period to protect many instances of short term value information.

Working with Security Classifications

27. Security classifications can be applied to any asset that has value to the business. This includes information in whatever form (but not the IT systems used to store or process classified information), items of equipment, hardware and other valuables. Classification markings should be clear and conspicuous, including any special handling instructions. Where it is impractical to apply a marking (e.g. on equipment), staff must be made aware of the protection and procedures required. Where an asset has inherent transferable value or the nature of the item dictates the need for special handling (e.g. firearms, toxic / atomic materials etc.), organisations must ensure that appropriate (in some cases, statutory) controls are in place to protect against compromise, loss or damage.

28. When working with information assets, the following points need to be considered:

- There is no requirement to explicitly mark routine OFFICIAL assets.
- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.
- When working with documents, classifications must be in CAPITALS at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions.
- Sensitive material published on intranet sites must also be clearly marked.
- It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable systems should compel users to select a classification before sending, e.g. via a drop-down menu.
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure, including release under FOIA or to the National Archives.
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing OFFICIAL and SECRET material must be covered by the higher marking (i.e. SECRET).
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail 'string' before they add to it and forward it on.
- In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement.
- Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics.

Valuing technology assets: Confidentiality, Integrity and Availability

29. ICT systems need to keep information confidential, but also maintain the integrity and availability of information and / or services. The degree of impact on the business from a loss of availability or integrity may vary and should be considered as part of a comprehensive risk assessment process that takes into account threat, vulnerability, likelihood and mitigations. 'HMG IA Standard Numbers 1 and 2 – Information Risk Management' describes the process of assessing and managing risk to ICT systems.

30. In certain contexts (e.g. nuclear or air safety), the loss or compromise of integrity or availability may be so catastrophic that enhanced controls to mitigate these risks will be required even if the likelihood seems slight. Moreover, there are statutory security requirements that must be upheld in number of specialist fields, such as atomic materials, air safety, firearms, and witness protection.

31. The compromise of a significant volume of data (e.g. personal data) is likely to have a higher impact than the loss of individual information assets, and may merit more restrictive handling controls. Likewise, the inter-connectivity of different data sets may allow more sensitive connections to be made by association. **Aggregation, accumulation and association** of data (within ICT systems and on removable media) must be carefully considered as part of the risk management process as additional protective controls may or may not be appropriate.

Physical Security: Risk Assessment Methodologies

32. Physical security controls for the protection of HMG assets should be applied according to layering principles. A risk assessment is required to determine applicable threats and risks.

33. Once the threat(s) to the information is/are understood, and prior to purchasing or deploying a new security system or product, an Operational Requirement (OR - a structured methodology for determining security requirements) should be undertaken. Best practice guidance is available in the CPNI 'Guide to Operational Requirements for Security Measures'.

34. Where assets require protection from surreptitious attack, the 'Security Assessment for Protectively Marked Assets' (SAPMA) risk assessment methodology should be completed to determine suitable additional security controls to prevent or detect compromise.

Legal Framework

The UK classification system operates within the framework of domestic law. This includes:

a. **Official Secrets Act 1989:** Damage assessment is a critical element of the OSA, most of the offences in which require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons notified under section 1 of the OSA; Crown servants; government contractors; and any person.

b. **Data Protection Legislation**: The handling of personal data must be in compliance with Data Protection legislation. The Data Protection Act 2018, however, contains a number of exemptions to some or all of the data protection principles and to other provisions such as the right of access to personal data. For example, the Act provides an exemption from many of the requirements of the Applied General Data Protection Regulation to safeguard national security. But note that, although the exemption is widely drawn, it is only available to the extent that it is required for the purpose of protecting national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with Data Protection legislation. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one applies. Departments and agencies should also have regard to Data Protection legislation, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

c. **Freedom of Information Act 2000:** Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

d. **Public Records Act 1967.** Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

Annex - Security Controls Framework

Version 1.1 – May 2018

Summary

This Annex to the Government Security Classifications policy (December 2012) describes the physical, personnel and information security controls required to provide a proportionate and robust level of protection for assets at each of the three classification levels (OFFICIAL, SECRET and TOP SECRET).

Within each level, assets must be protected to broadly consistent standards wherever they are collected, stored, processed or shared across HM government and with wider public sector and external partners. This consistency is essential to provide the confidence that underpins effective information sharing and interoperability between organisations.

The Annex is provided in three sections:

- **Part One – Threat Model and Security Outcomes:** providing the context and objectives underpinning risk management decisions.
- **Part Two – Working with HMG Assets:** typical security controls that individuals should apply when working with information (and other assets) at each classification.
- **Part Three – Protecting Assets and Infrastructure:** high level principles to help organisations determine appropriate security requirements for the protection of ICT infrastructure / services, and other assets.

This document should be read in conjunction with the detailed standards and guidance set out in the HMG Security Policy Framework (SPF).

Cabinet Office
April 2013

Part One - Threat Model and Security Outcomes

1. Security classifications indicate the sensitivity of information AND the typical controls necessary to defend HMG assets against a broad profile of applicable threats. Risk owners should appreciate that information classified at one level cannot be assured to be protected against the threat profile associated with a higher level of classification.

OFFICIAL

2. The OFFICIAL tier provides for the generality of government business, public service delivery and commercial activity. This includes a diverse range of information, of varying sensitivities, and with differing consequences resulting from compromise or loss. OFFICIAL information must be secured against a threat model that is broadly similar to that faced by a large UK private company. This anticipates defending data and services against compromise by attackers with bounded capabilities and resources, including (but not limited to): hactivists, single-issue political pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

3. This model does not imply that information within the OFFICAL tier will not be targeted by some sophisticated and determined threat actors (including Foreign Intelligence Services) who may deploy advanced capabilities. It may be. Rather, a risk based decision has been taken not to invest in controls to assure protection against those threats, i.e. proportionate not guaranteed protection.

4. Technical controls at this level will be based on assured, commercially available products and services, without need for any bespoke development. Whilst these controls cannot absolutely assure against the most sophisticated and determined threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.

SECRET

5. The SECRET threat model anticipates a higher level of threat capability than would be typical for the threat model described in the OFFICIAL tier. The model includes threat sources such as elements of serious and organised crime as well as some state actors. Attacks may be bespoke in nature and tailored to specifically attack the target infrastructure. Vulnerable elements of the supply chain may be targeted to facilitate a further compromise of information. The opportunities for accidental compromise of information will be minimised, with technical protection where possible.

6. Risk owners should appreciate that assured protection will not be provided against very sophisticated, persistent and blended attacks by the most capable and determined organisations (such as highly competent state actors). A level of risk acceptance is required, that these threat sources have the capability to successfully target information within this tier if they are motivated to do so.

TOP SECRET

7. The TOP SECRET threat model reflects the highest level of capability deployed against the nation's most sensitive information and services. Very little risk can be tolerated in this tier, although risk owners should note that no activity is entirely free from any risk.

Security Outcomes

To defend against these typical threat profiles, protective security controls should achieve the following outcomes at each classification level:

	OFFICIAL	SECRET	TOP SECRET
Outcome	• Meet legal and regulatory requirements • Promote responsible sharing and discretion • Proportionate controls appropriate to an asset's sensitivity • Make accidental compromise or damage unlikely	• Make accidental compromise or damage highly unlikely • Detect and resist deliberate attempts at compromise • Make it highly likely those responsible will be identified	• Prevent unauthorised access • Detect actual or attempted compromise • Identify those responsible and respond appropriately
Personnel Security	• Access by authorised individuals for legitimate business reasons	• Assurance that access is only by known and trusted individuals	• High assurance that access is strictly limited to known and trusted individuals
Physical Security (handling, use, storage, transport and disposal)	• Proportionate good practice precautions against accidental or opportunistic compromise • Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely	• Detect and resist deliberate compromise by forced and surreptitious attack • Destroy / sanitise to make reconstitution and / or identification of constituent parts highly unlikely	• Robust measures to prevent compromise by a sustained and sophisticated or violent attack • Destroy / sanitise to prevent retrieval and reconstitution

Information Security (storage, use, processing or transmission)	• Protect against deliberate compromise by automated or opportunist attack • Aim to detect actual or attempted compromise and respond.	• Detect and resist deliberate compromise by a sophisticated, determined and well resourced threat actors	• Robust measures to prevent compromise from sustained attack by sophisticated, determined and well resourced threat actors

Part Two: Working with HMG Assets

8. This section describes typical personnel, physical and information security controls required when working with HMG assets. The indicative controls table should be used as the basis for local security instructions and processes.

9. The identified controls are cumulative - minimum measures for each classification provide the baseline for higher levels.

10. Organisations may need to apply controls above (or below) the baseline to manage specific risks to particular types of information. Such exceptions must be agreed with the respective data owners and delivery partners. The Government SIRO will moderate any instances that entail pan-government risk.

11. Security requirements must be set out in local security instructions and reinforced by training to ensure that individuals understand their responsibilities. Organisations should operate an appropriate security culture commensurate with their particular circumstances and risk appetite.

12. HMG assets need to be managed to meet the following basic principles. More stringent controls may be appropriate to manage more sensitive assets:

    a. Handle with care to avoid loss, damage or inappropriate access. Compliance with applicable legal, regulatory and international obligations is the minimum requirement.

    b. Share responsibly, for business purposes. Use appropriately assured channels as required (e.g. internal HMG email) and provide meaningful guidance on specific sensitivities and handling requirements.

    c. Store assets securely when not in use. For example, implement clear desk policies and screens locking when ICT is left unattended.

    d. Where assets are taken outside the office environment they should be protected in transit, not left unattended and stored securely. Precautions should be taken to prevent overlooking or inadvertent access when working remotely or in public places.

    e. When discussing HMG business in public or by telephone, appropriate discretion should be exercised. Details of sensitive material should be kept to a minimum.

    f. Particular care should be taken when sharing information with external partners or the public; for example, emails, faxes and letters should only be sent to named recipients at known addresses.

    g. Information that is not freely available in the public domain should be destroyed in a way that makes reconstitution unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

    h. Report any incidents involving theft, loss or inappropriate access to HMG assets.

13. The below table describes standard control measures when working with information assets at each classification level. It should be read in conjunction with the detailed policy and guidance set out in the Security Policy Framework (SPF).

14. At OFFICIAL, the controls are recommended as good practice for all routine information, but organisations may want to adopt a more directive approach to control access to particularly sensitive information (e.g. information handled with the OFFICIAL-SENSITIVE caveat).

	OFFICIAL	SECRET	TOP SECRET
Personnel Security (Refer to the SPF Personnel Security paper for detailed guidance)	Minimum controls include: • Appropriate recruitment checks (e.g. the BPSS, or equivalent) • Reinforce personal responsibility and duty of care through training • 'Need to know' for sensitive assets	Additional minimum controls include: • Always enforce Need to Know • SC for regular, uncontrolled access • Special Handling Instructions	Additional minimum controls include: • DV for regular, uncontrolled access
Physical Security c. Document handling	• Clear desk / screen policy • Consider proportionate measures to control and monitor access to more sensitive assets	• Register and file documents in line with locally determined procedures • Maintain appropriate audit trails • Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission • Limit knowledge of planned movements to those with a need to know	• Register movement of documents and undertake annual musters • Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and record results • Strictly limit knowledge of planned movements to those with a need to know
d. Storage	• Storage under single barrier and / or lock and key • Consider use of appropriate physical security equipment / furniture (see the CPNI	• Defence in Depth • Use of CPNI Approved Security Furniture (refer to CSE) • Segregation of shared cabinets • Proportionate measures to control	• Robust measures to control and monitor movements • Information must be accountable

	‘Catalogue of Security Equipment’, CSE)	and monitor access / movements	
e. Remote Working	• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Store more sensitive assets under lock and key at remote locations	• Risk assessment to determine need and identify appropriate protective security controls • CPNI approved security furniture at remote location (see CSE) • Approval may need to be sought from the originator	• Only to be removed for remote working as an exception if determined essential and following acceptance of the inherent risks by senior management
f. Moving assets by hand:	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files	• Risk Assess the need for two people to escort the movement of document(s)/media • Documented local management approval required and completion of document / media removal / movement register • Sealed tamper-evident container / secure transportation products (refer to CSE) • Not accessed in public areas	• Senior Manager approval subject to risk assessment
g. Moving assets by post / courier	• Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier’s ‘track and trace’ service	• Local Management approval required, actions recorded in document movement register • Robust double cover • Approved registered mail service commercial courier (‘track and trace’), or Government courier	• Senior Manager approval subject to risk assessment • Special handling arrangements may need to be considered

h. Moving assets overseas (by hand or post)	• Trusted hand under single cover • Consider using reputable commercial courier's 'track and trace' service	• Trusted hand (appropriate security clearance, e.g. SC) • Sealed tamper evident container / secure transportation products (refer to CSE) • Where travelling to / via a country of 'Special Security Risk' the container should be carried by a diplomatically accredited courier	• Security cleared (DV) diplomatically accredited courier only
i. Bulk Transfers (Volume thresholds may vary by organisation and should be defined in local policies)	• Local management approval, subject to departmental policy, appropriate risk assessment and movement plans	• Senior management approval, subject to departmental policy, appropriate risk assessment and movement plans • Commercial companies could be used provided information transported in sealed containers/ crates, accompanied by departmental staff and movement and contingency plans are in place	• Local police aware of movement plan
INFORMATION SECURITY[1] a. Electronic Information at Rest	• Electronic Information will be protected at rest by default. This may be appropriate physical protection (such as data at rest in a government data centre) or may involve Foundation Grade data at rest encryption when physical control isn't guaranteed (such as on a laptop)	• Electronic Information will normally be protected at rest by physical security appropriate for SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with (revitalised) Enhanced Grade protection	• Electronic Information will normally be protected at rest by physical security appropriate for TOP SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with High Grade protection

1 NB. Information Security Controls are described in greater detail in part three of this annex.

b. Electronic Information in Transit	• Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption • Information may be emailed / shared unprotected to external partners / citizens, subject to local business policies and procedures • Where more sensitive information must be shared with external partners (e.g. citizens), consider using secure mechanisms (e.g. browser sessions using SSL / TLS)	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems
c. ICT Services	• Different GCloud services will be suitable for different types of OFFICIAL information. Risk owners MUST read and understand any GCloud accreditation residual risk statements • ICT services developed by a Department or delivery partner must follow the risk management processes as set out in HMG IA Standards IS1 and 2 and follow standard architectural	• ICT Services must be accredited as appropriate considering the SECRET threat model. CESG design patterns or bespoke advice may be required • Very careful risk assessment and understanding of implications of enabling functionality • Information exchange outside of the SECRET tier will be highly constrained and managed using shared accredited capability	• ICT systems designed must be accredited as appropriate considering the TOP SECRET threat model. Bespoke architectural advice may be necessary

	approaches • End user devices will conform to the security principles defined in the *End User Device (EUD) Strategy: Security Framework and Controls*		
d. Removable Media (data bearing)	• The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference • Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement • Consider appropriate encryption to protect the content, particularly where it is outside the organisation's physical control	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection
Telephony (mobile and landline), Video Conference and Fax	• Details of sensitive material should be kept to a minimum • Recipients should be waiting to receive faxes containing personal data and / or data marked with the OFFICIAL – SENSITIVE caveat	• Secure Telephony, VTC and secure fax	• Secure Telephony, VTC and secure fax
Disclosure	• Much of the information in this domain is likely to be releasable	• Likely to engage FOIA exemption in whole or in part (e.g. 23, 24, 26,	• Subject to a case by case assessment there is a general

(Statutory disclosures are separate from the classification scheme and require case-by-case assessment)	unless an FOI exemption is in force, it is personal data subject to Data Protection legislation or there is another statutory bar • Official Secrets Act (OSA) and criminal cases subject to damage tests. • Where appropriate, non-sensitive information should be published for reuse	27, 31), to be assessed on a case by case basis • Some information might be releasable in a securely redacted format	presumption that information is: • above the OSA Prosecution threshold • subject to FOIA exemptions on National Security (or other) grounds
Archiving and Transfer to The National Archives	• Transfer as open records wherever possible, at 20 years and in accordance with the Public Records Act	• Retain as long as classification level applies	• Retain as long as classification level applies
Disposal / Destruction	• Dispose of with care using approved commercial disposal products to make reconstitution unlikely (refer to CPNI guidance and HMG IS5.)	• Verify document is complete before destruction • Use approved equipment and or service providers listed in the CSE	• Control measures to witness / record destruction
	• Guidance about the physical destruction of assets is available in 'CPNI Requirements for Secure Destruction', March 2013. • Electronic media used to process HMG assets must be sanitised and disposed of in accordance with the requirements in 'HMG IA Policy No. 5 - Secure Sanitisation.'		
Incident Reporting	• Local reporting arrangements • Escalation to DSO and SIRO as appropriate for significant incidents • ICO notified of "significant" losses of personal data • GovCert / CINRAS for ICT incidents	• DSO and SIRO notified, local procedures followed • Consider notifying Accounting Officer and responsible Minister • ICO notified if personal information • May be appropriate for Police investigation subject to damage test and Cabinet Office gateway	• Accounting Officer, Minister and Cabinet Office alerted

		process	
	• Guidance about the management and handling of security incidents is available in the SPF documents 'Security Breach Management' and 'Leaks Procedural Guidance'. Relevant ICO guidance should also be consulted.		

Part Three – Protecting Assets and Infrastructure

15. This section is intended to help security practitioners and information risk professionals to determine appropriate security requirements for the protection of infrastructure, ICT systems / services, and other assets at each level of the classification system.

16. It outlines context, process and security considerations at a high level but cannot, of itself, provide the level of detail necessary to implement specific technical architectures or deploy a new security system or product. It must be read in conjunction with the detailed policy, guidance and structured risk assessment methodologies set out in the Security Policy Framework.

Physical Security Principles:

17. Physical security controls should be applied appropriately, mindful of the 'layering principles'. A risk assessment is required to determine the applicable threats and risks.

18. Once the threats to an asset are understood, and prior to purchasing or deploying a new security system, an 'Operational Requirement' (OR) should be completed to determine an appropriate blend of physical security controls (and counter-terrorism controls where applicable). The Catalogue of Security Equipment (CSE) lists suitable products, graded 'Base', 'Enhanced' or 'High' to reflect performance in resisting forced attack.

19. Where assets require protection against surreptitious attack (i.e. espionage), a 'Security Assessment of Protectively Marked Assets' (SAPMA) should be completed to determine whether additional security controls may be required. Appropriate products are detailed in the CSE, rated as CPNI Classes 1 to 4 to reflect the different levels of skill / knowledge of the attacker and the resources available to them.

20. Where it is not feasible to protect the entirety of a large or bulky item (e.g. tanks, aircraft, ammunition etc), the most sensitive elements of the item should be protected using appropriate CSE products. Enhanced procedural controls may also be appropriate, for example, additional vetting and / or guarding.

Information Security Principles

21. Information at any level of classification should receive broadly consistent levels of protection across the Public Sector. This consistency is essential to establish trust between organisations and promote greater interoperability.

22. The broad risk appetite for information types will be overseen by the appropriate pan-government governance body. For the OFFICIAL and SECRET tiers this will be the Senior Cyber and Risk Assurance Board (SCaRAB) and the Office of the Government SIRO (OGSIRO). For the TOP SECRET tier this will be the Information Sharing Policy Board (ISPB) and the SIA Release Authorities.

23. Public Sector organisations continue to own and manage their own information risk, within the bounds of the top level HMG risk appetite set by the SCaRAB / ISPB. Within this framework there remains an enduring requirement for organisations to assess their own information risks and make appropriate accreditation decisions which balance risk with realising business opportunities.

24. Departmental SIROs are responsible for managing Departmental risk with SCaRAB / ISPB responsible for shared or pan-Government risk. The OGSIRO should be consulted if local decisions exceed the HMG risk appetite (as set out in the *HMG Information Risk Directive*) AND there is a pan-government impact.

25. ALL Public Sector ICT systems must be appropriately accredited, although accreditation activities should be proportionate to the system functionality and level of information risk. Where shared services have existing or a community accreditation (e.g. the Public Services Network (PSN) and G-Cloud services), then Departments can rely on this assurance providing it supports their own risk appetite (including understanding of any documented residual risks). This supports the ICT Strategy Programmes "accredit once, use many" model.

Confidentiality, Integrity and Availability Considerations

26. The Classification Policy relates to Confidentiality requirements. However, Public Sector information and services often have significant Integrity and/or Availability requirements too. There exist many scenarios where the consequences of a loss of Integrity or Availability can be significantly more severe than a loss of Confidentiality.

27. A high Integrity or Availability requirement does not lead to a high classification. A holistic risk assessment must be conducted, which includes the consideration of risks to Confidentiality, Integrity and Availability respectively. Treatment of significant Integrity or Availability requirements may require robust technical controls and a high level of assurance, over and above that indicated by the (Confidentiality driven) classification.

Sensitive Information

28. Some particularly sensitive information will attract a Caveat (e.g. OFFICIAL-SENSITIVE) or Special Handling Instructions (e.g. CODEWORDS or National Caveats) to denote the need for further controls, particularly in respect of sharing. The impact of compromise of this information may be higher, but this does not imply that it will necessarily be subject to the threat model applicable to higher tiers.

29. Such information can be managed at the same classification level, but with a more prescriptive information handling model, potentially supported by extra procedural or technical controls to reinforce the need to know. The aim of additional technical controls is to manage the information characteristics that attract the additional marking (for example enforcing access control, or technically limiting the number of records a user can view). These controls will be data and system dependent.

Aggregation

30. As government employs greater sharing and reuse of commoditised ICT solutions as well as shifting public services delivery to online channels, there is potential for large volumes of data objects to be concentrated in a small number of systems or services, or for a single system to provide a large number of government services.

31. Aggregation of data or services may result in the following conditions being realised:

- The impact to the business from the loss, compromise or misuse of an aggregated data set is likely to be higher than the impact of compromise of a single object. The increase in impact can, under some circumstances, be severe (such as very large sets of citizen data);
- Existing Threat Sources will remain relevant but these threats may be more motivated to mount an attack as the benefit to them of compromising a large number of data objects is more appealing;
- Threat Sources may be attracted to attack the aggregated data set or service because the return on investment may be sufficiently increased. This is especially relevant when considering aggregation of value bearing transactions. These Threat Sources may therefore deem it worthwhile to deploy an increased technical capability.

32. Aggregated data sets should be considered to be within the same classification level; however where the impact of compromise or loss has increased as a result of aggregation, these aggregated data sets must be carefully and tightly controlled.

33. Aggregation of data at rest on end user devices, or the aggregated presentation of data to end user devices must be avoided as far the business requirement allows. This minimises the impact of compromise of the device or of inappropriate action from the user (accidental or malicious). This may include technical controls to physically limit the data or services being accessed, as well as transactional monitoring approaches to detect and respond to anomalous data or service access.

34. A risk assessment must be undertaken to determine the specific technical controls needed to protect the aggregated data set – this will include an understanding of how aggregation affects threat. Technical controls to protect an aggregated data set should be robust and risk owners may decide that they require a higher level of assurance or additional technical capability (such as fault tolerance). The risk assessment for the given aggregated service or data set should determine the specific technical controls within an appropriate architecture.

Assessing the impact on the Business [2]

35. Organisations are required to assess the potential impact to the business in the event that specific information risks are realised. This assessment should form part of a comprehensive risk assessment which also considers threat, vulnerability and likelihood.

[2] N.B. Work is underway to refocus business impact assessment as a qualitative process that forms part of the overall risk assessment. A transition plan for introducing the new process, terminology and rule set will be available by October 2013; this section will be updated in due course.

This risk assessment process considers Confidentiality, Integrity and Availability of information independently.

36. Within each tier there will be a range of information with varying degrees of business impact should the risks be realised – this is particularly true when considering the OFFICIAL tier.

37. The existing Business Impact Level (BIL) structure should continue to be used in the course of an information risk assessment process. BIL's should not on their own be used to 'label' information systems or indicate a level of accreditation. In due course the BIL policy will be revised to provide a qualitative assessment process that supports the genuine business priorities. There is no direct mapping between existing BILs and any given classification.

Security Enforcing Functionality

38. Where any security functionality or security product is relied upon, there must be confidence that those products or functions are effective and are providing the protection that is expected of them. All such products must therefore have an appropriate level of independent validation or assurance, proportionate to the classification of the information they are used to protect.

Information Assurance Policy and Guidance

39. Information Assurance Standards and good practice guidance set out in the HMG Security Policy Framework (SPF), as well as additional products in CESG's IA Policy Portfolio, remain extant. Many of these documents describe good practice which is agnostic of classification labels.

40. Documents that specifically reference the former Government Protective Marking System (GPMS) and/or BILs will over time be updated or withdrawn. In the interim period 'transition' guidance will be available to help organisations use the existing good practice advice with the new Classification Policy.

Technical Controls Summary

OFFICIAL

41. ALL HMG information assets have value and require an appropriate level of protection, whether in transit, at rest or whilst being processed. Pan-government interoperability and trusted sharing are founded on mutual assurance that organisations apply consistent risk management approaches and that information will receive broadly equivalent levels of protection. At OFFICIAL, a de facto common baseline of protection is provided through a framework of controls:

    - Any legal obligations (e.g. DPA) or regulatory requirements;
    - The broad risk appetite for OFFICIAL, set out in the *HMG Information Risk Directive;*
    - SPF policy and guidance, including this Control Framework, HMG Information Assurance Standards and CESG's good practice guidance;
    - Common assurance and accreditation processes, including the Baseline Control Set (BCS);
    - Common security compliance regimes (e.g. GSI / PSN Codes of Connection);
    - UK Government Reference Architecture;
    - Common trusted infrastructure offerings delivered through the ICT Strategy programmes (End User Devices, Public Services Network, G-Cloud and G-hosting), noting that any residual risks should be managed in line with local risk appetites;
    - HMG ICT Moratorium and Spend Controls Processes.

42. There is a diverse range of government business and information at OFFICIAL. Within this broad framework, there is an onus on risk owners to understand the business value and sensitivity of their information and the ways in which they work with and share it. This will determine specific Confidentiality, Availability and Integrity requirements that manage the precise risks to any particular asset within the OFFICIAL baseline.

43. OFFICIAL information will normally be protected utilising appropriately assured, commercially available security products and service offerings. Government will not seek to create bespoke products or ICT services to manage information risk at this level.

44. Where assurance of security enforcing functionality is required, products should be certified against the relevant Security Characteristics for that class of product. Assurance will normally be delivered through industry led (but independent) assessments under the CESG Commercial Product Assurance (CPA) scheme (Foundation Grade), though other assurance processes may be appropriate following a suitably scoped risk assessment or validation exercise.

45. Whilst Foundation Grade security product assurance or service offerings will be industry led, some CESG oversight may be appropriate where these products or services are being provisioned to, for example, a sufficiently sized proportion of the Public Sector as to present a 'national level' of risk.

46. OFFICIAL information will be accessed and shared using a variety of methods, including the internet, GSi and PSN. Information in transit should be protected by default, unless there are sensible business reasons where this is not appropriate and the business can tolerate the risk. In practice, use of encryption would be expected to secure (for example) the following information exchanges:

    - OFFICIAL data at rest on End User Devices and removable media;
    - Remote access connections and sessions (e.g. VPN) into secure environments such as a corporate network or cloud service;
    - Transactional services (e.g. payment services) delivered to the citizen over untrusted networks;
    - Connections between networks or interconnections within a geographically separated network – i.e. at the infrastructure (not user) level, between Public Sector organisations[3];
    - Information that relates to or directly supports National Security.

47. There is no policy requirement to encrypt routine (email) information exchanges with external partners (citizen, industry, local government, third sector). However, where sensitive information (or routine personal data) is exchanged over untrusted infrastructure with external partners, consideration should be given to protecting it using technologies such as client-side email encryption, or providing access to information via a secure browser session, (such as an individual using SSL/TLS to view online banking information or webmail).

48. Service offerings supporting the OFFICIAL tier will be commercially based. These services could be delivered by industry (with industry led independent assessment), or developed as a Public Sector service but still utilising commercial technologies. Organisations will have to make risk informed decisions as to what type of service is appropriate based on their business requirements. For example, the business requirement to host a public information service will necessitate the use of a different type of service offering, from a requirement to process personal medical data. Security enforcing products within the service offering would be expected to be independently validated or assured as described above.

49. Public Sector organisations will increasingly be expected to utilise shared services delivered through pan-government ICT programmes. These programmes will provide a range of commoditised products and service offerings, with different security characteristics and levels of assurance. Organisations that plan to utilise these shared services and infrastructure to manage assets at OFFICIAL must read the detailed technical standards and guidance developed for the relevant programme, along with any statements of residual risk associated with the use of a particular product or service:

[3] NB. Encryption is increasingly becoming standard commercial practice to protect information in transit. It is anticipated that the availability of standard, easy to deploy and use encryption technology will lead to a future standard encrypted PSN, where encryption does not attract a cost premium. This single, protected environment will in future make secure interoperability straightforward and intuitive for the Public Sector.

Public Services Network (PSN)

50. The ICT Strategy anticipates that the PSN will be the primary network bearer for OFFICIAL information. PSN consuming organisations must comply with the *PSN IA Conditions*, and manage any stated residual risks inline with local risk appetites.

End User Devices (EUD)

51. The EUD programme anticipates that any OFFICIAL information (including information handled with the OFFICIAL-SENSITIVE caveat) can be managed on a single device that conforms to the security principles defined in the *End User Device Strategy: Security Framework and Controls*, (March 2013). Note that the assurance required (including compliance with relevant legislation such as Freedom of Information Act (FoIA) and DPA), means that EUDs will normally be owned, managed and controlled by the organisation. Any stated residual risks must be managed in line with local risk appetites.

G-Cloud

52. The G-Cloud programme anticipates that most OFFICIAL information can be managed through accredited service offerings available via the CloudStore. Service offerings will be accredited according to *G-Cloud Information Assurance Requirements and Guidance,* and any stated residual risks should be managed in line with local risk appetites. Three types of service are defined, that will likely be appropriate for different types of information and business processes:

    - Unassured Cloud services. These services (formerly Impact Level 00x) may be appropriate for a limited amount of information where there is no Confidentiality requirement (such as marketing and communications data intended for public consumption), although risk owners should consider whether they have Integrity or Availability requirements that must be managed.
    - Assured Public Cloud (formerly Impact Level 22x) services will be subject to a suitably scoped ISO27001 certification and other assurance activities as described in the *GCloud Information Assurance Requirements and Guidance.* Such services may be appropriate for the generality of OFFICIAL information, although organisations should carefully consider the scope of the IS027001 certification, the geographic location of the hosting, and any other residual risks identified as part of the G-Cloud Accreditation Statement. It is unlikely that these services will be suitable for more sensitive information.
    - Formally accredited Public Cloud (formerly Impact Level 33x) or Private Cloud services will be subject to a full HMG accreditation and will be hosted within the UK. These services are likely to be appropriate for most OFFICIAL information, although organisations should still be mindful of any risks involved in outsourcing services and data to the cloud (including those set out in the G-Cloud Accreditation Statement).

53. Organisations that are considering utilising G-cloud service offerings must note the following:

    - Off-shoring of information that relates to or supports National Security is prohibited.
    - The Office of the Government SIRO must review any plans to off-shore HMG data. Wherever possible, any personal data held off-shore should be kept within the EEA,

under the EU-US Privacy Shield Framework or the limited number of countries with positive findings of adequacy from the European Commission.

Data Centre Consolidation:

54. The Data Centre Consolidation Programme (G-Hosting) anticipates reducing the number of Government (and public sector) data centres through a programme of virtualisation, consolidation and rationalisation. Security and resilience requirements for data centres will be determined on a site specific basis, aligned to broader initiatives to ensure appropriate protections for Critical National Infrastructure (CNI) assets.

SECRET

55. SECRET information must be very well protected against the defined threat model. The SECRET tier will be a largely isolated trust domain with only specific and assured information exchange functionality to less trusted domains.

56. SECRET ICT infrastructure will be physically or cryptographically isolated from less trusted domains (such as OFFICIAL ICT systems or the Internet). The only exceptions to this requirement will be:

- Gateways that provide specific business information exchange functionality. These gateways will require appropriate architectural assurance and as far as possible represent shared capability.
- At the discretion of SCaRAB where there is an overwhelming business requirement. Specific arrangements will be necessary to manage urgent operational imperatives.

57. Products protecting SECRET information will provide very robust protection that includes holistic security controls. The appropriate level of product assurance at SECRET is a revitalised and strengthened Enhanced Grade Standard; this will include a broader set of data separation technologies in addition to cryptography.[4]

58. The model for SECRET includes very sensitive information that is subject to a sophisticated threat, but much SECRET information doesn't carry an enduring long-term intelligence life. For some SECRET information that is very sensitive and is of enduring intelligence value, risk owners should carefully consider whether this information should in fact reside in the TOP SECRET tier.

TOP SECRET

59. High Grade assurance remains appropriate for TOP SECRET tier protection. This level of assurance will support UK sovereignty requirements.

[4] NB. More detailed information about the technical controls required for the protection of SECRET and TOP SECRET information will be set out in additional, classified guidance.

Publication date: October 2013

© Crown copyright 2013
You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence or email psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk

You can download this publication from www.gov.uk.