Cabinet Office

v.4.0
May 10

HMG Security Policy Framework

Making government work better

Contents Page

HMG Security Policy Framework

Foreword by Sir Gus O'Donnell

Effective security is central to how we handle many of the challenges facing Government. It is vital for public confidence and for the efficient, effective and safe conduct of public business.

Responsibility for security is delegated down from the Prime Minister and Cabinet to me, as Head of the Home Civil Service and chairman of the Official Committee on Security, and then to Heads of Department. Ultimately, however, security is the responsibility of everyone and our policies and processes will only work well if we all play our part.

The new Security Policy Framework replaces the Manual of Protective Security and the Counter-Terrorist Protective Security Manual. It sets out universal mandatory standards, as well as offering guidance on risk management and defining new compliance and assurance arrangements. For the first time the framework allows for much of this material to be placed in the public domain, allowing greater access, increasing awareness, transparency and sharing good practice.

The framework introduces changes in the way we do things, as part of our broader agenda to modernise and transform Government. Work to modernise security policy and processes will continue: to raise awareness, ensure that guidance is up to date, that policy reflects changes in threat and circumstance, and that Departments are supported from the centre.

I am confident that this framework will enable Government to do its job better and I commend it to all in the public service.

Gus O'Donnell

Introduction

The Security Policy Framework (SPF) represents a new and innovative approach to protective security and risk management in government. The SPF has a solid policy basis, taking and adapting much of the Manual of Protective Security (MPS) and the Counter-Terrorist Protective Security Manual (CTPSM).

Whilst much of the existing policy within those manuals has found its way into the new framework, it must be noted that the SPF represents a new approach. It is vital that organisations understand that the SPF cannot simply be applied as their own departmental security policy, but that it must be used, adapted and applied in framing departmental security policies to meet the specific business needs of the organisation and its delivery partners.

In general terms the framework is aimed primarily at Government Departments and Agencies in supporting its protective security and counter-terrorism responsibilities; however, it does have wider application. The commercial sector plays an increasingly intimate role within the UK government matrix, as well as making up the core sectors within the Critical National Infrastructure (energy, water, agriculture, etc). Similarly, organisations such as the National Health Service, Police forces and local Government all handle government assets on a regular basis.

It should be noted for contractual purposes that any general reference to MPS or CTPSM should now be considered as the SPF. As there have been no fundamental changes in policy it is felt that there should be no requirement to re-negotiate existing contracts on this basis.

The SPF has four tiers, or levels, each representing a key element (of increasing detail) within the Government's protective security system. First and foremost, is that security not only supports business goals, but must proactively be considered a business enabler, making government work better, safer and more confidently. Next are a set of five core security principles, highlighting accountability at senior levels, collective responsibility of all staff and contractors, and the need to employ trustworthy people. At the third tier is a series of concise key policy documents, which clearly identify (by highlighting in green boxed text), the minimum mandatory requirements. These standards include the new 'Data Handling Procedures in Government' published by Cabinet Office in June 2008, which have now been formalised into a new Information Assurance Standard (IA Standard no.6); 'Handling Personal Data and Managing Information Risk. It is important to stress here that these are the minimum requirements; it is expected that many Departments and Agencies will manage their specific security risks over and above these baseline measures, using sound risk management principles as outlined within the framework.

These higher levels, particularly tier three, provide the fundamentals of security policy and represent the essence of the framework. They have been made publicly available (http://www.cabinetoffice.gov.uk/spf) representing our commitment to transparency and openness, but also and perhaps more importantly, to support a cultural shift required to ensure that security and risk management are given sufficient prominence in all areas and at all levels of business across Government.

The tier four level of the framework is aimed primarily at the security practitioner; containing an assortment of detailed technical standards, supplementary policy and guidance, as well as references to other security and risk management websites and organisations. Much of this material is protected and will only be made available to those who have a legitimate 'need to know' through secure web access. However, where there is universally applicability, added value, and no increase in vulnerability, material has been made publicly accessible at this level. Tier 4 provides the tools to support the core policy and principles, the material will be fluid, being up dated regularly to meet specific vulnerabilities and adapted to the changing threat picture.

To this extent the principles, core values and minimum requirements expressed within the SPF are highly and widely applicable.

Compliance arrangements and assurance mechanisms are based around three elements: self assessment, central reporting and internal audit. Departments and Agencies will continue to decide on their own arrangements for assuring themselves of their security standards and the SPF provides guidance on this; however, Departments will also be required, in the form of an annual security assessment, to report to Cabinet Office on compliance with the minimum mandatory requirements. Further assurance is provided by internal audit committee's recognition of the SPF, and that the policies therein can inform internal audit assessment programmes. It must be noted that any weakness or non-compliance will need to be addressed in the Departmental Statement of Internal Control; a publicly available document.

The information collected by the Cabinet Office annual security assessment, will, along with other data, be used to inform an annual Security report to the Official Committee on Security, (SO) chaired by the Cabinet Secretary.

This has been a truly collective and co-ordinated exercise, drawing on technical policy and operational experts from across the security community. Particular thanks must go to the Centre for Protection of National Infrastructure (CPNI), based within the Security Service and the National Technical Authority for Information Assurance (CESG) based within the Government Communication Headquarters, who have provided expertise and support to the Cabinet Office's Government Security Secretariat .

Overarching Security Statement

Protective Security, including physical, personnel and information security, is an essential enabler to making government work better. Security risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

Core Security Principles

1. Ultimate responsibility for HMG security policy lies with the Prime Minister and the Cabinet Office. Departments and Agencies, via their Permanent Secretaries and Chief Executives, must manage their security risks within the parameters set out in this framework, as endorsed by the Official Committee on Security (SO).

2. All HMG employees (including contractors) have a collective responsibility to ensure that government assets (information, personnel and physical) are protected in a proportionate manner from terrorist attack, and other illegal or malicious activity.

3. Departments and Agencies must be able to share information (including personal data) confidently knowing it is reliable, accessible and protected to agreed standards irrespective of format or transmission mechanism.

4. Departments and Agencies must employ staff (and contractors) in whom they can have confidence and whose identities are assured.

5. HMG business needs to be resilient in the face of major disruptive events, with plans in place to minimise damage and rapidly recover capabilities.

Security Policy No.1: Governance, Risk Management and Compliance

1. This is the first of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Governance

2. Governance arrangements for security rely on the partnership between the centre of Government, Departments and Agencies, their delivery partners, individuals working in the security community, and ultimately all staff employed on behalf of HMG. The role of Cabinet Office at the centre of Government is to provide leadership and co-ordination of shared risks (such as asset control and vetting) by setting policy and overseeing regulation. Departments are responsible for the protection and utilisation of their assets – information, personnel and physical – as appropriate to their business needs and circumstance. Departments are best placed to assess the risks they face, and must develop their own security policies in line with this framework. It is for the Centre to set minimum measures, providing an agreed level of protection and assurance across Government.

3. The Security Policy Framework (SPF) outlines mandatory security policy requirements that all Departments and Agencies must meet. This framework should also be extended, where necessary, to any organisations working on behalf of, or handling HMG assets, such as Non-Departmental Public Bodies (NDPBs), contractors, Emergency Services, devolved administrations, Local Authorities, or any regular suppliers of goods and / or services. In areas where statutory security requirements apply (e.g. air safety, nuclear security) this framework must be applied in line with those requirements. Departmental Security Officers (DSOs) (in consultation with the Senior Information Risk Owner (SIRO) as necessary) will need to determine where and what level of compliance is required of their delivery partners, and where equivalent security policies are acceptable. This policy is supplemented by detailed advice and guidance which the DSO can distribute on a 'need to know' basis.

MANDATORY REQUIREMENT 1

Departments and Agencies must ensure that all staff understand the relevant requirements and responsibilities placed upon them by the Security Policy Framework and that they are properly equipped to meet the mandatory security policies (green boxes) as set out in this framework.

Where Departments, Agencies and their contractors are subject to statutory security requirements, such requirements shall take precedence. The requirements set by security regulators and actions carried out by them will be consistent with this framework.

MANDATORY REQUIREMENT 2

Departments must ensure that their Agencies and main delivery partners are compliant with this framework, and must consider the extent to which those providing other goods and / or services to them, or carrying out functions on their behalf, are required to comply.

Cabinet Office leadership

4. The Official Committee on Security (SO) is responsible for formulating security policy and coordinating its application across government. SO is also the National Security Authority for dealing with international organisations such as NATO and the EU. Cabinet Office Government Security Secretariat (COGSS) provides the secretariat for SO and is responsible for developing and communicating this framework, ensuring compliance with the minimum requirements, supporting Departments and preparing an annual report to SO on the state of security across Government. COGSS works closely with the security and intelligence community in developing and reviewing security policy.

Roles, accountability and responsibilities

5. Whilst security is a collective responsibility for all staff and contractors, ultimate responsibility for security rests with Ministers, Permanent Secretaries, and / or other Accounting Officers and their respective Management Boards which must include a Senior Information Risk Owner (SIRO). Cabinet Office will write to newly appointed Heads of Department setting out their responsibilities with regard to security – the Head of Department/Permanent Secretary is

ultimately accountable for security within their Department. The Prime Minister and the Cabinet Secretary have ultimate responsibility for ensuring overall coherence of security across Government, and that security objectives are met.

MANDATORY REQUIREMENT 3
Departments must have a stated Board level representative responsible for security (e.g. Head of Department/Permanent Secretary). Departments must identify clearly where security responsibilities lie, including the relationship between the Department's main Board and the Boards of their Agencies or other bodies.

MANDATORY REQUIREMENT 4
Departments and Agencies must have a designated Departmental Security Officer (DSO), with day-to-day responsibilities for all aspects of Protective Security (including physical, personnel and information security).

6. In addition to the mandatory roles above, and those outlined within Security Policy No. 4: Information Security and Assurance (see MR 35; organisations need to consider appropriate roles within their security/business machinery. For example larger bodies may consider appointing Deputies and / or creating other specific security roles (e.g. Personnel Security Officer), whilst smaller bodies may combine roles. Agencies may wish to consider their parent departmental DSO as their designated DSO. The Head of Department/Permanent Secretary has overall responsibility for security and it is for them to determine appropriate security structures within their organisation and any Agencies for which they are responsible.

Risk management

7. Departments need to 1) identify their assets and those responsible for them, 2) understand the vulnerability and likelihood of attack from various threats, 3) value them in terms of the impact from loss or failure of confidentiality, integrity and availability, and 4) assign a proportionate level of protection to mitigate, and / or recover from, the potential loss or failure of those assets. Departments should see this as a continuous cycle of assessing and re-evaluating risk.

8. Departments should use the HM Treasury Orange Book on Risk Management for a broad approach to principles and concepts, however, within the disciplines of Information Assurance and Counter-Terrorism Protective Security there are detailed methods of risk assessment that must be adopted (see Security Policy No. 4 – Information Security and Assurance and Security Policy No. 6 – Counter-Terrorism for these areas).

MANDATORY REQUIREMENT 5

Departments and Agencies must adopt a risk management approach (including a detailed risk register) to cover all areas of protective security across their organisation.

Assurance

9. Self-assessment, central reporting, audit and review, must combine together to provide for a robust level of assurance across Government, as well as assisting the centre in developing and refining policy.

Self assessment

MANDATORY REQUIREMENT 6

Departments and Agencies must:

a) Make their departmental security policy widely available internally and reference this in overall business plans.

b) Have a system of assurance of compliance with security policy, and produce an annual report to their Head of Department / Management Board on the state of all aspects of protective security.

10. Departments should include details of any agencies or other bodies that report to them directly in the annual report to their Head of Department.

Central reporting

MANDATORY REQUIREMENT 7

Departments must submit an annual security return to the Cabinet Office Government Security Secretariat, covering their Agencies and main delivery partners, and must include:

a) Details of any changes to key individuals responsible for security matters (The appointment of a new DSO must be reported immediately).

b) Significant departmental risks and mitigations that have implications for protective security.

c) All significant security incidents (those involving serious criminal activity, damage to National Security, breaches of international security agreements, serious reputational damage, notifiable data losses or leaks) – individual breaches of this nature must also be reported immediately.

d) Declaration of the level of compliance against each Mandatory Requirement (green boxes).

e) Confirmation that any significant control weaknesses have been reflected in the Departmental Statement on Internal Control.

Audit and review

11. Departments will be responsible for carrying out internal reviews of security arrangements as they judge to be necessary. The Cabinet Office, in consultation with Departments and the Official Committee on Security, will review compliance as appropriate on the basis of the minimum mandatory requirements (green boxes) and annual security returns.

MANDATORY REQUIREMENT 8

Departments and Agencies must comply with oversight arrangements including external audit / compliance arrangements as set out by Cabinet Office.

Culture, training and professionalism

12. Fostering a professional culture and developing a positive attitude toward security is critical to the successful delivery of this framework. Security must be seen as an integral part of and a

key enabler to, effective departmental business. Cabinet Office, in conjunction with professional bodies such as the Centre for Protection of National Infrastructure (CPNI) and CESG, the National Technical Authority for Information Assurance, maintain a programme of familiarisation, training and re-fresher courses appropriate for security personnel, including an induction visit to all new DSOs. Departments and Agencies must ensure that regular refresher training, awareness programmes and security briefings are provided to all staff. These should cover individual security responsibilities, as defined by the Civil Service Code, including the reporting of security incidents and criminal behaviour and / or any knowledge of leaking. In addition to line management reporting, all staff must also have recourse to consult with, or report anonymously to a welfare officer or independent arbiter.

MANDATORY REQUIREMENT 9

Departments and Agencies must ensure that:

a) Board members responsible for security undergo security and risk management familiarisation upon appointment.

b) All DSOs are given a joint security briefing from Cabinet Office and the Centre for Protection of National Infrastructure (CPNI) on appointment, and have either attended the relevant training courses before, or at the earliest opportunity after appointment.

c) All Departmental Security Unit (DSU) staff possess competencies and training to the appropriate level, either by attending relevant internal departmental or external government training.

d) Security education and awareness must be built into all staff inductions, with regular familiarisation thereafter.

e) There are plans in place to foster a culture of proportionate protective security.

f) There is a clearly stated and available policy, and mechanisms in place, to allow for independent and anonymous reporting of security incidents.

International security agreements

13. HMG is party to a range of multilateral and bilateral international security agreements governing the protection, handling and use of classified material. These agreements commit parties to apply equivalent, mutually agreed security standards for the protection of classified material; including personnel, information and industrial security

14. Departments and Agencies engaged in sensitive work with international organisations, or those that handle classified information on their behalf, must ensure that their internal procedures are compliant with all relevant international obligations (e.g. NATO, EU etc.).

MANDATORY REQUIREMENT 10

Departments and Agencies must ensure that they adhere to any UK obligations as set out in this framework and governed by multilateral or bilateral international security agreements.

15. Where no such agreements are in place, Departments as Agencies must ensure that foreign classified information held by them is protected to the same standard as equivalent UK information.

Security Policy No.2: Protective Marking and Asset Control

1. This is the second of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Introduction

2. The Protective Marking System (often referred to as the Government Protective Marking System/Scheme or GPMS) is the Government's administrative system to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction. The system is designed to support HMG business, and meet the requirements of relevant legislation, international standards and international agreements.

MANDATORY REQUIREMENT 11

Departments and Agencies must apply the Protective Marking System and the necessary controls and technical measures as outlined in this framework.

Legal requirements

3. The Official Secrets Acts 1911 to 1989 (OSAs), and the Data Protection Act 1998 (DPA) impose statutory obligations regarding the protection and handling of official information and of personal data respectively. In contrast, the Freedom of Information Act 2000 (FOIA) establishes a statutory regime for the release of information held by public authorities to any person requesting it. Both FOIA and DPA are subject to a number of important exemptions, which apply for example, to material which may prejudice law enforcement or damage national security if disclosed. All staff who handle government material must have an understanding of this legislation and how it specifically relates to their role. The Protective Marking System is an administrative system designed to protect information (and other assets) from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence, and must therefore be viewed against the legal background.

MANDATORY REQUIREMENT 12

Departments and Agencies must provide all staff with guidance on the Official Secrets Acts, Data Protection Act and Freedom of Information Act. Staff handling protectively marked information must be given guidance on how this legislation relates to their role.

Official Secrets Acts

4. Sections 1 to 6 of the Official Secrets Act 1989 (OSA 1989) contain a range of offences concerning damaging disclosures of information, documents or other articles. These criminal prohibitions are aimed primarily at those in Government service, although they are equally applicable to anyone else in receipt of official information (whether or not as a result of an unauthorised disclosure). The OSA 1989 makes no reference to the Protective Marking System, but does specify the categories of interests to which damage must, or must potentially, be caused by the unauthorised disclosure. These are: 1) Security and intelligence; 2) Defence; 3) International relations; 4) Foreign confidences; 5) Crime; 6) Special investigation powers.

5. Members of the security and intelligence services, by virtue of Section 1(1) of the OSA 1989, are subject to an absolute prohibition against unauthorised disclosure of information, or other assets relating to security or intelligence regardless of whether or not it is a damaging disclosure. Similarly, any persons who are 'notified' under Section 1(1) of the OSA (because, for example, they have regular access to information relating to security or intelligence) are subject to the same prohibition. It should also be noted that it is an offence to disclose information or assets which it would be reasonable to expect might be used to obtain access to information protected under the Act (e.g. access codes, passwords, keys, etc).

6. Departments must assess whether, by virtue of their roles and responsibilities, any of their staff or contractors are notifiable under Section 1(1) of the Official Secrets Act 1989. Cases of doubt should be referred to the Government Security Secretariat for guidance. Any organisation responsible for notified employees or individuals must ensure they are notified in writing. These organisations must:

a) Renew notices every five years.

b) Keep under review the need for continuing notification of individual posts.

c) Maintain and keep under review the number of notifiable posts.

MANDATORY REQUIREMENT 13 – Not in use.

Data Protection Act 1998 (DPA)

7. Compliance with data protection legislation requires appropriate management structure and control. Proper application of the Protective Marking System will also ensure that protectively marked personal information is appropriately safeguarded and that requirements of the DPA are met. Section 7 of the DPA entitles an individual to be informed whether their personal data is being processed by the data controller, and to be given access to that personal data (a subject access request). This right is subject to exemptions for specified categories of information as defined by the Act. Whilst the DPA makes no reference to the Protective Marking System, protective markings may be a helpful indicator that an exemption applies. The presence, or absence, of a protective marking is not in itself a deciding factor as to whether or not information should be released in response to a subject access request, but it may nevertheless provide some initial guidance as to whether and which exemption applies.

MANDATORY REQUIREMENT 14

Departments and Agencies must follow the minimum standards and procedures for handling and protecting citizen or personal data, as outlined in HMG IA Standard No.6 - Protecting Personal Data and Managing Information Risk.

Freedom of Information Act

8. The Freedom of Information Act 2000 (FOIA) gives any person the right to request and be provided with information held by public authorities, although exemptions apply to specific information as defined by the Act. Whilst FOIA makes no reference to the Protective Marking System, protective markings may be a helpful indicator that an exemption applies. However, the presence, or absence, of a protective marking is not the deciding factor as to whether information should be released or not under FOIA. It should also be noted that the protective marking may no longer be current, and, while it reflects the highest classification of the information contained in a document, the file may also contain information that is not sensitive and may be subject to disclosure in a redacted form.

9. Under FOIA the holder of the information is responsible for answering a request for information; however, if the holder is proposing to disclose protectively marked information, the originator, or specified owner of the information must be consulted before disclosure. When a classified document has been released under FOIA it should be marked accordingly, for example, 'Released under FOIA in full on [date]'.

10. Foreign FOI legislation, where it exists, can differ from the UK; therefore the 'UK' prefix must be used when sending protectively marked material abroad. The onus is on those sending the material to seek to ensure that any UK protectively marked material is not subject to release under foreign FOI legislation unless by prior agreement.

11. Departments must consult the Ministry of Justice FOI Clearing House (clearinghouse@justice.gsi.gov.uk; 020 3334 3891) for guidance about any FOI requests that concern information supplied by or relating to bodies dealing with security matters (section 23), National Security (section 24), or any other triggers for automatic referral. This includes any requests concerning protectively marked information originating from an overseas government or international organisation (or commercial entity). Where possible, the originator or specific UK departmental owner must also be consulted when considering the request.

MANDATORY REQUIREMENT 15
Departments and Agencies must ensure that any protectively marked material that is to be released under the Freedom of Information Act is de-classified first and is marked as such. The originator, or specified owner, must be consulted before protectively marked material can be de-classified.

The 'need to know' principle

12. The effective use (including the sharing and protection) of information is a key priority for Government. Access to sensitive information or assets will be required for the efficient management of HMG business. However, access must only be granted to those who have a business need and the appropriate personnel security control (BPSS or National Security Vetting).This 'need to know' principle is fundamental to the security of all protectively marked Government assets – casual access to protectively marked assets is never acceptable. If there

is any doubt about giving access to sensitive assets individuals should consult their managers or security staff before doing so.

MANDATORY REQUIREMENT 16
Departments and Agencies must ensure that access to protectively marked assets is only granted on the basis of the 'need to know' principle. All employees must be made fully aware of their personal responsibility in applying this principle.

International security standards

13. The Government Protective Marking System is designed to meet the principles of the international standard on Information Security Management Systems (ISO/IEC 27000 series). This standard represents good practice to which this framework is aligned. More details are to be found in Security Policy No.4 - Information Security and Assurance and a copy of ISO/IEC (27001) is reproduced as a supplement to this framework.

International markings

14. Classified assets originated by international organisations and foreign governments that the UK has agreements with should be afforded the same level of protection as its equivalent UK protective marking. See MR10.

MANDATORY REQUIREMENT 17 – Not in use.

Material originating outside of HMG

15. Outside HMG there is no agreed UK system for marking sensitive material, although terms such as PRIVATE and CONFIDENTIAL are in common use, particularly in relation to personal information. Any material originating outside of government, that is not covered by a recognisable protective marking, international agreement, contract or other arrangements, but is marked in such a way to indicate sensitivity, must when handled by HMG, be protected to at least the level offered by the PROTECT marking, and a higher marking should be considered.

MANDATORY REQUIREMENT 18

Departments and Agencies must ensure that non-HMG material which is marked to indicate sensitivity is handled at the equivalent level within the Protective Marking System, or where there is no equivalence, to the level offered by PROTECT as a minimum.

The Government Protective Marking System

16. The Protective Marking System comprises five markings. In descending order of sensitivity they are: **TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT**. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed. These markings can be applied to any government assets, although they are most commonly applied to information held electronically or in paper documents. The methodology used to assess these principles within information systems is expressed in Business Impact levels.

Universal controls

17. There are a number of specified technical controls for each level of protective marking. The controls below apply to all protectively marked information.

MANDATORY REQUIREMENT 19

Departments and Agencies must apply the following baseline controls to all protectively marked material:

a) Access is granted on a genuine 'need to know' basis.

b) Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer etc) staff must still have the appropriate personnel security control and be made aware of the protection and controls required.

c) Only the originator or designated owner can protectively mark an asset. Any change to the protective marking requires the originator or designated owner's permission. If they cannot be traced, a marking may be changed, but only by consensus with other key recipients.

d) Assets sent overseas (including to UK posts) must be protected as indicated by the originator's marking and in accordance with any international agreement. Particular care must be taken to protect assets from foreign Freedom of Information legislation by use of national prefixes and caveats or special handling instructions.

e) No official record, held on any media, can be destroyed unless it has been formally reviewed for historical interest under the provisions of the Public Records Act.

f) A file, or group of protectively marked documents or assets, must carry the protective marking of the highest marked document or asset contained within it (e.g. a file containing CONFIDENTIAL and RESTRICTED material must be marked CONFIDENTIAL).

Applying the correct protective marking

18. The originator or nominated owner of information, or an asset, is responsible for applying the correct protective marking. When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required. The 'harm test' should be done by assessing the asset against the criteria for each protective marking.

19. If applied correctly, the Protective Marking System will ensure that only genuinely sensitive material is safeguarded. The following points should be considered when applying a protective marking:

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business.
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset.
- The compromise of aggregated or accumulated information of the same protective marking is likely to have a higher impact (particularly in relation to personal data). Generally this will not result in a higher protective marking but may require additional handling arrangements. However, if the accumulation of that data results in a more sensitive asset being created, then a higher protective marking should be considered.

- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.

20. The criteria below provide a broad indication of the type of material at each level of protective marking. Detailed requirements, including specific details on definitions, protection, handling and disclosure instructions are contained in supplementary material within the framework.

Criteria for assessing **TOP SECRET** assets:

- **threaten directly the internal stability of the United Kingdom or friendly countries;**
- **lead directly to widespread loss of life;**
- **cause exceptionally grave damage to the effectiveness or security of United Kingdom or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;**
- **cause exceptionally grave damage to relations with friendly governments;**
- **cause severe long-term damage to the United Kingdom economy.**

Criteria for assessing **SECRET** assets:

- **raise international tension;**
- **to damage seriously relations with friendly governments;**
- **threaten life directly, or seriously prejudice public order, or individual security or liberty;**
- **cause serious damage to the operational effectiveness or security of United Kingdom or allied forces or the continuing effectiveness of highly valuable security or intelligence operations;**
- **cause substantial material damage to national finances or economic and commercial interests.**

Criteria for assessing **CONFIDENTIAL** assets:

- **materially damage diplomatic relations (i.e. cause formal protest or other sanction);**
- **prejudice individual security or liberty;**
- **cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;**
- **work substantially against national finances or economic and commercial interests;**
- **substantially to undermine the financial viability of major organisations;**
- **impede the investigation or facilitate the commission of serious crime;**
- **impede seriously the development or operation of major government policies;**
- **shut down or otherwise substantially disrupt significant national operations.**

Criteria for assessing **RESTRICTED** assets:

- **affect diplomatic relations adversely;**
- **cause substantial distress to individuals;**
- **make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;**
- **cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies;**
- **prejudice the investigation or facilitate the commission of crime;**
- **breach proper undertakings to maintain the confidence of information provided by third parties;**
- **impede the effective development or operation of government policies;**
- **to breach statutory restrictions on disclosure of information;**
- **disadvantage government in commercial or policy negotiations with others;**
- **undermine the proper management of the public sector and its operations.**

Criteria for assessing **PROTECT** (Sub-national security marking) assets:

- **cause distress to individuals;**
- **breach proper undertakings to maintain the confidence of information provided by third parties;**
- **breach statutory restrictions on the disclosure of information;**
- **cause financial loss or loss of earning potential, or to facilitate improper gain;**
- **unfair advantage for individuals or companies;**
- **prejudice the investigation or facilitate the commission of crime;**
- **disadvantage government in commercial or policy negotiations with others.**

Special handling

21. Supplementary markings may be applied to protectively marked material to indicate additional information about its contents, sensitivity and handling requirements. These markings can include national caveats (e.g. UK EYES ONLY), descriptors, codewords or compartmented handling regimes. In most cases, special handling requirements are only applied to highly sensitive material (e.g. intelligence material or material marked CONFIDENTIAL and above).

MANDATORY REQUIREMENT 20

Departments and Agencies must meet special handling arrangements where they apply and ensure that all staff handling such information understand these arrangements.

Breaches

22. Departments and Agencies must present their staff with a clear indication of the incremental penalties for breaching the rules regarding protectively marked material and the other mandatory requirements as laid out in this framework. This must include recourse to disciplinary and, where applicable, criminal proceedings.

MANDATORY REQUIREMENT 21

Departments and Agencies must have a breach system and give clear guidance to all staff that deliberate or accidental compromise of protectively marked material may lead to disciplinary and / or criminal proceedings.

Security Policy No.3: Personnel Security

1. This is the third of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Purpose

2. The purpose of personnel security is to provide a level of assurance as to the trustworthiness, integrity and reliability of all HMG employees, contractors and temporary staff. As a minimum requirement all staff are subject to recruitment controls known as the Baseline Personnel Security Standard (BPSS). For more sensitive posts there are a range of security controls, referred to as 'National Security Vetting' (NSV): these are specifically designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

Risk management

3. Departments and Agencies must employ a risk management approach to Personnel Security in conformity with protective security principles, seeking to reduce the risk of damage, loss, or compromise of HMG assets by application of personnel security controls before and during employment. These controls do not provide a guarantee of reliability and must be supported by effective line management, nor should they be considered an alternative to the correct application of the 'need to know' principle or to access and information security controls.

MANDATORY REQUIREMENT 22

Departments and Agencies must, as part of their risk management approach to protective security, assess the need to apply personnel security controls against specific posts and the access to sensitive assets.

Personnel security controls

Baseline Personnel Security Standard (BPSS)

4. The BPSS is the recognised standard for HMG pre-employment screening. It forms the foundation for National Security Vetting and seeks to address identity fraud, illegal working and deception generally. The BPSS comprises verification of four main elements: 1) identity; 2) employment history; 3) nationality and immigration status (including the right to work); and, if a formal NSV clearance is not required for the post, 4) unspent criminal records. In addition, prospective employees are required to account for any significant periods spent abroad. Satisfactory completion of the BPSS allows regular access to UK RESTRICTED and UK CONFIDENTIAL assets, and occasional access to UK SECRET assets, provided an individual has a 'need to know'.

MANDATORY REQUIREMENT 23
Departments and Agencies must apply the requirements of the Baseline Personnel Security Standard (BPSS) to all HMG staff (including the armed forces), and contractors and temporary staff.

5. In some cases, such as people taken on for very short periods of employment, or where local personnel are recruited overseas, it may not be practicable to meet the BPSS fully. In these instances the decision to accept the risk must be recorded. Verification of identity and right to work is a prerequisite that must be completed before the UK security clearance process is undertaken.

National Security Vetting

6. National Security Vetting is governed by HMG's statement of policy, made by the Prime Minister to Parliament on 15 December 1994. There are three levels of National Security Vetting: Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). The need for vetting must be assessed against the requirements of each particular post. Vetting is required for those who have unescorted access to sites or work in close proximity to individuals

assessed to be at risk of terrorist attack, who have access to information or assets which may be of value to terrorists, or have constant and frequent access to SECRET and /or TOP SECRET information or other assets, including the protectively marked assets of other nations and international organisations, the compromise of which could bring about the same degree of damage.

7. National Security Vetting involves a degree of intrusion into an individual's private life and must only be applied in accordance with HMG's statement of policy. For legal and policy reasons, it is not available on demand or on a speculative basis.

MANDATORY REQUIREMENT 24

Departments and Agencies must ensure that National Security Vetting is only applied where it is necessary, proportionate and adds real value.

National Security vetting procedures

MANDATORY REQUIREMENT 25

Departments and Agencies must follow the procedures for National Security Vetting as contained in supplementary material within the framework.

8. Permission for the relevant checks to be carried out is provided by an individual completing and signing a Security Questionnaire, indicating that they have read and understood HMG's policy statement on security vetting. It must be counter-signed by an appropriate member of staff from the sponsor organisation, indicating that checks are required for national security purposes. All organisations undertaking security vetting must ensure that they are covered by the provisions of the Security Service Act 1989 (Section 2(3)).

National Security Vetting decisions

9. In making vetting decisions, judgement must be exercised taking into consideration all the information obtained during the clearance process. The existence of one or more factors of concern does not necessarily or conclusively demonstrate unreliability or present an unmanageable risk. Vetting officers must take into account the nature, likelihood and credibility of the threat, and the vulnerability, sensitivity and impact of compromise of the particular assets

concerned, as well as any mitigating factors. They must also make every effort to establish the facts and resolve any apparent discrepancies which are revealed, or doubts which arise before making a clearance decision. When a security risk is identified the vetting authority must decide whether or not the risk is manageable, and if so, provide advice to line management, taking into account that information may have been revealed or obtained in confidence.

MANDATORY REQUIREMENT 26

Only Government Departments and Agencies, or Police Forces can take security clearance decisions. They must make clear evidence based decisions taking into account all available information. They must be prepared to defend a decision if challenged.

Refusal or withdrawal of clearance

10. If a clearance is refused or withdrawn for an existing HMG employee or a contractor, the Department or Agency must inform the individual of the fact and provide full reasons for that decision, unless there are demonstrable national security grounds for non-disclosure of the reasons. There is no requirement to inform applicants for employment (staff or contractors) of the fact or reasons for the refusal of a clearance, but this may be possible allowing for considerations of security and confidentiality, as it may impact on future employment applications.

Ongoing personnel security management ('Aftercare')

11. Personnel security is an important element of an effective protective security regime as well as good overall management practice. The security clearance process only provides a snapshot of an individual at a particular time. The BPSS and National Security Vetting are the beginning of an ongoing and actively managed personnel security regime, which requires senior and line management support, awareness and education, and formal periodic reviews of security clearance.

MANDATORY REQUIREMENT 27

Departments and Agencies must have in place personnel security aftercare arrangements, including formal reviews of National Security Vetting clearances and the requirement to remind managers and individuals of their responsibility to inform the vetting authorities of any change in circumstance that may impact on the suitability to hold a security clearance.

Appeals

12. Existing employees must be made aware of the organisation's internal appeals process, and, if the decision to refuse or withdraw clearance is upheld, of the option to appeal to the independent Security Vetting Appeals Panel (SVAP). The Panel is available to all those, other than external applicants for employment, in the public and private sectors and in the Armed Forces who are subject to National Security Vetting, have exhausted existing internal appeal mechanisms within their organisations and remain dissatisfied with the result. Individuals must be provided with details of how to apply to the Panel and be informed that appeals must be received within 28 days of the individual being informed of the internal appeal decision. In all such cases Departmental legal advisers must be consulted. The Security Vetting Appeals Panel will make recommendations to the Head of Department, who will take the final decision as to whether clearance is granted or not. Departments and Agencies should be aware that individuals may also seek to challenge vetting decisions through legal avenues.

13. External applicants for employment are not eligible to appeal against adverse vetting decisions either internally or to the SVAP. Separate arrangements are available to applicants to, and staff and contractors of the Security and Intelligence Agencies through the Investigatory Powers Tribunal (IPT).

MANDATORY REQUIREMENT 28

Departments and Agencies must have in place an internal departmental appeals process for existing employees wishing to challenge National Security Vetting decisions.

MANDATORY REQUIREMENT 29

Departments and Agencies must inform Cabinet Office Government Security Secretariat where an individual initiates a legal challenge in respect of a National Security Vetting decision.

Assurance

MANDATORY REQUIREMENT 30

Departments and Agencies must record how many, and what type of security vetting clearances (CTC, SC, DV) have been undertaken on an annual basis, and also the number, and the outcome of, internal and independent vetting appeals. This should be included in the annual report to your Head of Department / Management Board.

Security Policy No.4: Information Security and Assurance

1. This is the fourth of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Introduction

2. Information is a key asset to Government and its correct handling is vital to the delivery of public services and to the integrity of HMG. Departments need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed. As our reliance on cyber space continues to increase, so do the number and complexity of associated security challenges. The global reach, relatively low cost and anonymity of the cyber domain means that those posing a threat ranges from hostile states and terrorists, to criminals and low level hackers. The way we view and approach information security must be cognisant of this dynamic and pervasive cyber environment.

Information security policy

MANDATORY REQUIREMENT 31

Departments and Agencies must have, as a component of their overarching security policy, an information security policy setting out how they, and their delivery partners (including offshore and nearshore (EU/EEA based) Managed Service Providers), comply with the minimum requirements set out in this policy and the wider framework.

Managing information risk

3. In striking the right balance between sharing and protecting data, Departments and Agencies must manage business impacts and risks associated with Confidentiality, Integrity and Availability (C, I & A) of all information. Information Assurance (IA) is the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. The IA functions that support the protection of Government Information and Communications Technology (ICT) Systems are risk

management, accreditation, standards and compliance. The importance of IA to public service delivery has been demonstrated by the publication of a National IA Strategy; this policy supports this strategy. The International Standard for Information Security Management Systems (ISO/IEC 27001) is acknowledged as good practice and this policy is aligned to that standard.

MANDATORY REQUIREMENT 32
Departments and Agencies must conduct an annual technical risk assessment (using HMG IA Standard No.1) for all HMG ICT Projects and Programmes and when there is a significant change in a risk component (Threat, Vulnerability, Impact etc.) to existing HMG ICT Systems in operation. The assessment and the risk management decisions made must be recorded in the Risk Management and Accreditation Documentation Set (RMADS), using HMG IA Standard No.2 - Risk Management and Accreditation of Information Systems.

4. When handling personal data there is a further requirement to conduct a risk assessment every quarter, please refer to HMG IA Standard No.6 – Protecting Personal Data and Managing Information Risk.

Business impact

5. In assessing the level of impact likely to result from any compromise of information assets, Departments and Agencies must use 'Business Impact Levels', also known simply as Impact Levels (ILs) (IL 0 - no impact, to IL6). ILs provide a seven-point scale which allows Departments and Agencies to make a balanced assessment of the countermeasures to meet risk management requirements for Confidentiality, Integrity and Availability. In addition, organisations must review where large amounts of data are aggregated, accumulated, or associated with other data, to determine whether a higher Impact Level, and therefore greater protection and specific handling, is required.

MANDATORY REQUIREMENT 33

Departments and Agencies must, in conjunction with the Protective Marking System, use Business Impact Levels (ILs) to assess and identify the impacts to the business through the loss of Confidentiality, Integrity and/or Availability of data and ICT systems should risks be realised. Aggregation of data must also be considered as a factor in determining ILs.

Personal data

6. HMG must handle, protect and share large amounts of personal data to maximise public service delivery. Departments and Agencies must comply with the data protection principles set out in the Data Protection Act to ensure a high level of confidence that personal data is handled correctly. There are specific requirements relating to handling personal data as defined in HMG IA Standard No.6 – Protecting Personal Data and Managing Information Risk – see Mandatory Requirement 13.

Roles and responsibilities

7. Accounting Officers (e.g. Head of Department/Permanent Secretary) have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This responsibility must be supported by a Senior Information Risk Owner (SIRO) and the day-to-day duties may be delegated to the Departmental Security Officer (DSO), IT Security Officer (ITSO), Information Asset Owners (IAOs), supported by the Lead Accreditor.

MANDATORY REQUIREMENT 34

Information risk must be specifically addressed in the departmental annual Statement on Internal Control (SIC), which is signed off by the Accounting Officer.

MANDATORY REQUIREMENT 35

Departments and Agencies must have:

a) A designated Senior Information Risk Owner (SIRO); a Board level individual responsible for managing departmental information risks, including maintaining and reviewing an information risk register (the SIRO role may be combined with other security or information management board level roles).

b) A designated Lead Accreditor (LA), responsible for ensuring the accreditation process meets HMG IA Standards Nos 1 and 2.

c) A designated Information Technology Security Officer (ITSO); responsible for the security of information in electronic form.

d) A designated Communications Security Officer (ComSO) if cryptographic material is handled.

e) Information Asset Owners; senior named individuals responsible for each identified information asset.

8. It is advised that the ITSO reports to the DSO on information security matters. Where this is not the case, there should be clear mechanisms to ensure that IT security is considered as part of the overall approach to protective security. Similarly it is advised that the Lead Accreditor reports to the SIRO on IA matters. Smaller Departments and Agencies may wish to combine ComSO and ITSO roles, while larger ones may consider appointing Deputies and / or creating other specific IT/Communications security posts. It is also sufficient for Agencies to consider parent Departmental roles as their designated SIRO/ITSO/IAO/LA/ComSO.

Accreditation and audit

9. Formal accreditation and audit processes provide important assurances that necessary standards are being met. As well as overall compliance arrangements for protective security (set out in Security Policy No.1: Governance, Risk Management and Compliance), there are specific and mandatory Information Assurance accreditation requirements.

MANDATORY REQUIREMENT 36

ICT systems that process protectively marked Government data must be accredited using HMG IA Standard No. 2 - Risk Management and Accreditation of Information Systems, and the accreditation status must be reviewed at least annually to judge whether material changes have occurred which could alter the original accreditation decision.

MANDATORY REQUIREMENT 37

Departments and Agencies must have the ability to regularly audit information assets and ICT systems. This must include:

a) Regular compliance checks carried out by the Lead Accreditor, ITSO etc. (documented in the RMADS audit of the ICT system against configuration records).

b) A forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes.

MANDATORY REQUIREMENT 38

All ICT systems must have suitable identification and authentication controls to manage the risk of unauthorised access, enable auditing and the correct management of user accounts.

Codes of connection and technical controls

MANDATORY REQUIREMENT 39

Departments and Agencies must follow the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories (for example Government Secure Intranet (GSI)).

Codes of connection should cover the following technical policies:

a) **Patching policy, covering all ICT systems including Operating System and applications, to reduce the risk from known vulnerabilities.**
b) **Policy to manage risks posed by all forms of malicious software ('malware'), including viruses, spyware and phishing etc.**
c) **Boundary security devices - (e.g. firewalls) must be installed on all systems with a connection to untrusted networks, such as the Internet.**
d) **Content checking/blocking policy.**
e) **Lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access and functionality) than required.**

Where these are not covered by codes of connection, or Departments are not signatories, separate policies covering these areas must be established.

Cryptography

MANDATORY REQUIREMENT 40

Departments and Agencies must comply with HMG IA Standard No.4 – Communications Security and Cryptography (parts 1-3) for the protection of protectively marked material. Paying particular attention to the circumstances when encryption is required, the requirement to only use CESG approved solutions, the control mechanisms for cryptographic items, and the requirement for specified levels of personnel security clearance for individuals handling cryptographic items.

Eavesdropping and Electro-Magnetic Countermeasures

MANDATORY REQUIREMENT 41

Departments and Agencies must follow specific Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations.

Remote working/mobile media

10. Home or remote working will introduce new vulnerabilities associated with off-site and portable ICT devices and media (e.g. laptops, PDAs, mobile phones, memory sticks, external drives, MP3s etc). Departmental standards and guidelines must be used for connecting to public (insecure) ICT systems such as the internet. Departments and Agencies should also, when handling personal data, avoid where possible the use of mobile media.

MANDATORY REQUIREMENT 42

Departments and Agencies must have a policy on remote working (e.g. home or mobile) that complies with the requirements in this framework.

Procurement

MANDATORY REQUIREMENT 43

Departments and Agencies must ensure that security requirements are specified in ICT contracts and all new ICT contracts handling personal data must adhere to the Office of Government Commerce (OGC) ICT model terms and conditions.

Reporting incidents

MANDATORY REQUIREMENT 44

Departments and Agencies must have clear policies and processes for reporting, managing and resolving ICT security incidents. All security incidents must be reported to:

a) Appropriate departmental security authorities.

b) HMG incident management bodies: GovCERT for network incidents and CINRAS for communications security (involving CESG approved cryptographic items).

c) The Information Commissioner's Office and Cabinet Office Information Security and Assurance (IS&A) for significant actual or possible losses of personal data.

Cyber Security Operations Centre (CSOC)

11. In addition to the mandatory reporting channels listed in MR 44 the Cyber Security Operations Centre (CSOC) has a key role in actively monitoring the health of cyber space and in identifying, and coordinating the UK response to, cyber security incidents. The primary objective of the CSOC is to co-ordinate stakeholder activity (interfacing primarily with the relevant UK CERTs including GovCERT, CSIRTUK and MODCERT) and to assist stakeholders in providing a satisfactory, coherent response. Impact levels of an incident will be assessed using HMG IA Standard No.1. It is not intended that CSOC deal directly with the customers of a stakeholder, or disrupt any other pre-existing relationships. CSOC is accountable to the Office of Cyber Security (OCS) within Cabinet Office and, ultimately, to the Cyber Security Oversight Board in fulfilling this role.

Secure disposal

MANDATORY REQUIREMENT 45

Departments and Agencies must ensure that all media used for storing or processing protectively marked or otherwise sensitive information must be disposed of or sanitised in accordance with HMG IA Standard No. an 5 – Secure Sanitisation of Protectively Marked or Sensitive Information.

Personnel and physical security

12. Personnel and physical security are integral elements in mitigating information risk. Whilst the standards outlined in Security Policy No. 3 - Personnel Security and Security Policy No. 5 – Physical Security deal with these, it should be noted that ICT and cryptographic posts (e.g. ITSO, LA, Crypto-custodians and system administrators) must be specifically evaluated to assess the level of security clearances required. Moreover, the physical security of ICT hardware and infrastructures must be specifically addressed.

MANDATORY REQUIREMENT 46

Departments and Agencies must ensure that ICT users with higher levels of privilege and/or potentially wide access (e.g. system administrators, architects, programmers etc.), or those with responsibility for ICT security, must be subject to evaluation for National Security clearances appropriate to the protective marking of the information processed and the need to have access to sensitive background information from the central authorities.

MANDATORY REQUIREMENT 47

Departments and Agencies must ensure that all locations where information and system assets (including cryptographic items) are kept must have an appropriate level of physical security as set out in this framework.

Education, training and awareness

MANDATORY REQUIREMENT 48

Departments and Agencies must ensure that all users of ICT systems are familiar with the security operating procedures governing their use, receive appropriate security training, and are aware of local processes for reporting issues of security concern. They must further ensure that staff who manage and maintain the secure configuration of ICT systems, and those with access to information assets, are appropriately trained, are aware of incident reporting, and the minimum standards relating to the handling of protectively marked data.

Business Continuity and Disaster Recovery Planning

MANDATORY REQUIREMENT 49

Departments and Agencies must ensure that all locations where information and system assets (including cryptographic items) are kept must have appropriate Business Continuity and Disaster Recovery Plans.

13. These plans should form part of overall Business Continuity plans - see Security Policy No. 7 – Business Continuity and MR 70 or details.

Security Policy No.5: Physical Security

1. This is the fifth of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Purpose

2. Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorised access and protection of HMG assets – information, personnel and physical. This means putting in place, or building into design, measures that prevent, deter, delay and detect, attempted or actual unauthorised access, acts of damage and/or violence, and triggers an appropriate response. For example, effective perimeter fencing and heightened access control measures may deter an attack because of the difficulties of gaining access; CCTV, intruder alarms and Radio Countermeasures might detect an attack in progress and trigger interception; whilst vehicle stand-off, blast resistant glazing and postal screening can minimise the consequences of an attack. For detailed guidance on counter terrorist policy, please refer to Security Policy No. 6 – Counter-Terrorism.

Defence in depth

3. Physical security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security, which must take account of the balance between prevention, protection and response. Physical security measures, or products such as locks and doors, are categorised according to the level of protection offered.

4. The 'layered' approach to physical security starts with the protection of the asset at source (e.g. creation, access and storage), then proceeds progressively outwards to include the building, estate and perimeter of the establishment. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter should also be considered. To ensure appropriate physical security controls, departments must consider the following factors:

- The impact of loss of the site or asset.
- The level of threat.
- The vulnerability.
- The value, protective marking or amount of material held.
- The particular circumstances of the establishment, including considerations of environment, location and whether occupancy is sole or shared.

MANDATORY REQUIREMENT 50

Departments and Agencies must adopt a 'layered' approach to physical security, ensuring that their physical security policy incorporates identifiable elements of prevention, detection and response.

Storage of sensitive assets

5. Critical, sensitive or protectively marked assets should be protected against surreptitious attack. They should be located in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.

MANDATORY REQUIREMENT 51

Departments and Agencies must use the Physical Security Assessment Questionnaire and the Physical Security Baseline Controls Matrix to identify appropriate physical security measures to protect against the compromise of an asset (typically Protectively Marked Material) through covert or surreptitious means.

Secure containers

MANDATORY REQUIREMENT 52

Departments and Agencies must ensure that protectively marked or valuable material is secured in appropriate security containers. Large amounts of protectively marked material or equipment, which cannot be stored in a security container, must be stored in a secure room.

Secure rooms

6. Where there is a need to store large amounts of inherently valuable removable items, a Strong Room should be used.

MANDATORY REQUIREMENT 53
Departments and Agencies must ensure that windows, doors, locks and entry controls meet appropriate security standards in rooms holding protectively marked material or sensitive assets.

Office areas

7. A clear desk policy is recommended in all office areas (particularly in open plan or shared office areas). This is primarily to ensure that sensitive material is not left unattended. Where it is not possible to implement a full clear desk policy, a risk-based approach should be adopted and the decision recorded in the appropriate Risk Register. The same principle should apply to computer screens and other office areas used to display potentially sensitive information, such as walls, pinboards etc. Computer screens should not be sited where they could be illicitly viewed (e.g. overlooked by windows or reflective surfaces).

MANDATORY REQUIREMENT 54
In office areas (particularly open plan and shared areas); Departments and Agencies must put in place procedures to avoid access to protectively marked material by individuals who do not have a 'need to know'.

Building security

8. For the purpose of assessing security risks to a building, buildings are rated according to their level of resistance to forced or surreptitious attack and blast protection. In any building in which protectively marked or other valuable assets are stored, there should be as few points of exit and entry as the functions of the site and safety will allow. Where these exist, physical security controls, such as window bars, grilles, shutters, security doors etc, should be installed. The effectiveness of such controls may be enhanced by the use of intruder detection systems or guard services.

9. When choosing from the many physical security measures available, Departments should ensure that security controls are able to mitigate violent acts and deter, detect or delay intrusion - those who are not deterred should be forced to use tools and methods that facilitate detection and delay.

MANDATORY REQUIREMENT 55
Departments and Agencies must assess the security risks to their estate ensuring that security is fully integrated early in the process of planning, selecting, designing and modifying their facilities.

Physical access control

10. Access control refers to the practice of controlling and monitoring access to a property or asset. Physical access control can be achieved through a combination of manned guarding, and mechanical or technical means. When deciding which access control measures to deploy, Departments must ensure that they consider the security measures in an integrated manner, such as combining automated access control systems with photo passes and CCTV.

11. Frontline staff such as security guards and receptionists play a vital role in controlling access, but to be fully effective, they may need to be supported by:

- Automatic Access Control System (AACS)
- Pass or ID system
- Visitor control
- Pass activated doors, turnstiles etc
- Entry and exiting searching
- CCTV

12. Frontline staff are likely to be exposed to a higher level of risk than others. This should be considered in the risk assessment and additional protections should be put in place as required.

MANDATORY REQUIREMENT 56
Departments and Agencies must control access to their estate using safeguards that will prevent unauthorised access.

MANDATORY REQUIREMENT 57
Departments and Agencies must have plans and procedures for dealing with and intercepting unauthorised visitors or intruders. Such plans must include the ability to systematically search the establishment if necessary.

MANDATORY REQUIREMENT 58
Departments and Agencies must ensure that access control policies are made available to all staff, and that staff are briefed on their personal responsibilities (e.g. wearing a pass at all times, escorting visitors and searching their work area if required).

Incoming mail and deliveries

13. Delivered items can include letters, packets and parcels and may contain:

- explosive or incendiary devices
- blades or sharp items
- offensive materials
- chemical, biological or radiological (CBR) materials or devices.

14. Anyone receiving a suspicious delivery is unlikely to know exactly which type it is, so procedures should cater for every eventuality.

MANDATORY REQUIREMENT 59
Departments and Agencies must have appropriate procedures in place for screening incoming mail/deliveries for suspicious items.

Manned guarding

15. Manned guarding is a key element of integrated physical security. Guards provide deterrence against hostile activity and facilitate a rapid response to security incidents.

16. Guards may either be directly employed by a government department or agency, or be employed by a commercial guard force. Guard duties and the need for, and frequency of, patrols should be decided by considering the level of threat and any other security systems or equipment that might already be in place.

MANDATORY REQUIREMENT 60
Departments and Agencies must consider the use of guard forces to protect the assets they hold. Where guards are deployed the GSZ Manned Guarding Services Manual is considered best practice.

Perimeter security

17. A perimeter may be defined by a natural boundary, vehicle barriers such as bollards, by free-standing fences or walls, or by the outer walls of a building or divisions inside it. The security function of a perimeter is to provide a degree of physical, psychological and / or legal deterrence to intrusion, as well as providing a defined scope of physical responsibility.

MANDATORY REQUIREMENT 61
Departments and Agencies must establish a secure perimeter, with appropriate security barriers and entry controls. Perimeters should offer physical protection from unauthorised access, damage and interference and allow for the quick identification of suspicious individuals or unusual items.

18. A perimeter's effectiveness as a security measure can be enhanced by the deployment of Perimeter Intruder Detection Systems (PIDS), Closed Circuit Television (CCTV), security lighting and / or guard forces. Perimeters can also be strengthened, particularly against vehicle borne threat, by installing more robust fencing or other barrier systems. In deciding which

perimeter security measures to deploy, Departments and Agencies must ensure that they consider the security measures in an integrated manner. Security lighting is a relatively effective and low cost deterrent but the use of more expensive systems, such as PIDS and CCTV, should be considered when a higher level of protection and detection is required.

MANDATORY REQUIREMENT 62

Departments and Agencies must produce a detailed Operational Requirement before deciding to deploy a security measure, particularly when purchasing a system or security product. This should clearly define what the system is expected to achieve.

CCTV

MANDATORY REQUIREMENT 63

The deployment of CCTV must be in accordance with the Data Protection Act 1998.

19. Departments and Agencies should be particularly aware of the Data Protection Act Principles and the Information Commissioner's Code of Practice on CCTV, which is published under the Act.

Security Policy No.6: Counter-Terrorism

1. This is the sixth of seven Security Policies within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) **must** adhere.

Introduction

2. Departments and Agencies are responsible for managing their assets – information, personnel and physical. This includes reducing risk from terrorist attack to as low a level as is reasonably practicable. Here it is important to recognise that the visible level of security is a factor in terrorist targeting. Departments have legal obligations to protect employees and visitors. Departments must be resilient in the face of an attack and have in place physical security measures, proportionate to the threat and the assets to be protected and also contingency arrangements to facilitate the quick resumption of vital services (including contracted services). HMG is perceived by many terrorist groups as an attractive and 'legitimate' target, it is therefore of critical importance that Departments meet the obligations outlined in this framework.

CONTEST strategy

3. CONTEST is the Government's long term strategy for reducing the risk to the UK and its overseas interests from international terrorism. The strategy was published in July 2006 and more details can be found at: http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/#

Risk management

4. Departments must employ a risk management approach to Counter-Terrorism (CT) protective security, although it is recognised that for certain areas (for example the protection of nuclear weapons and nuclear materials) CT security policy will be intentionally more prescriptive. It should be noted that CT measures are likely to complement other security measures and therefore should be considered in conjunction with general protective security

risk management (please see Security Policy No. 5 – Physical Security and Security Policy No.7 – Business Continuity). However, there are some very specific baseline CT measures that all Departments must take and these are outlined in this Policy.

Categorisation of the government estate

5. All Departments should be considered a potential target for terrorist attack or hostile interest. Government establishments fall into three risk categories according to the likelihood of being a target of a terrorist attack. These risk categories are HIGH, MODERATE, and LOW.

MANDATORY REQUIREMENT 64

All Government establishments must be categorised according to the likelihood of being, or in close proximity to, a potential terrorist target.

Threat Levels

6. Threat Levels are designed to give a broad indication of the likelihood of a terrorist attack. The Threat Levels are LOW, MODERATE, SUBSTANTIAL, SEVERE and CRITICAL. The five levels reflect an assessment of probability of attack based on an analysis of terrorists' intentions, targeting priorities, capabilities and any evidence of current planning and timescales. Information on the national Threat Level is available on the Security Service website.

Threat information and briefings

7. If an establishment is identified as being at immediate threat, the police and security authorities will inform the Department and may take control of the scene. This can be either pre or post-incident depending on circumstances and may require careful handling to avoid compromising intelligence. In order to ensure Departments have current information on the terrorist threat, the Centre for the Protection of the National Infrastructure (CPNI) and Cabinet Office Government Security Secretariat (COGSS) produce regular threat updates, some of which can only be seen on a 'need to know' basis.

Government Estate Response Level system

8. The Cabinet Office operates a system of response giving Departments a broad indication of the level of protective security readiness required at any one time. The Response Level is informed by the level of threat as well as specific assessments of vulnerability and risk to HMG but Response Levels tend to relate to sites, whereas Threat Levels usually relate to broad areas of activity. The three Response Levels are: NORMAL, HEIGHTENED and EXCEPTIONAL.

9. Precise measures adopted for each individual site and at each Response Level are the responsibility of Departmental Security Officers (DSOs) in consultation with CPNI and specialist Counter-Terrorist Security Advisers, and must form part of CT planning. Measures are likely to include restricting access, increasing patrols and frequency of bag searching, however a more detailed description of incremental security measures is set out in the supplementary material within the framework.

MANDATORY REQUIREMENT 65

Department Security Officers must ensure that the Department and its Agencies have baseline Counter - Terrorist physical security measures and Counter - Terrorist incremental security measures in place at each Response Level.

Further, at each Response Level, DSOs must ensure that the identified Counter - Terrorist incremental security measures are applied.

Departments must be ready to impose or remove those measures with immediate effect when there is a change in Response Level and ensure that all staff are made clearly aware of the current Response Level and what Counter - Terrorist physical security measures must be adopted.

Counter-Terrorist protective security policy and plans

10. Departments are best placed to assess the risks they face, and must develop their own security policies in line with this Framework, as set out in Security Policy no.1. This must include an overarching Counter-Terrorist protective security policy providing management direction for the Department's CT effort.

MANDATORY REQUIREMENT 66

Departments and Agencies must, as part of their overall protective security policy, have a Counter-Terrorist protective security policy in place. This must seek to deter and minimise impact of an attack or hostile interest, and must include:

a) Application of central advice and guidance.

b) Departmental roles and responsibilities (including third parties, contractors etc).

c) Management controls and assurance that appropriate measures and plans are in place.

d) Communication arrangements including briefing of staff.

e) Arrangements for testing Counter-Terrorist plans.

f) Liaison with emergency services and any multi-agency contingency plans.

11. Departments must produce Counter-Terrorist contingency plans setting out the appropriate procedures to be followed in the event of an incident or imminent terrorist threat. CT contingency plans should be developed in accordance with national security authorities' advice and in consultation with local emergency services and should form part of departmental business continuity plans.

MANDATORY REQUIREMENT 67

All Government establishments that are assessed to be a HIGH or MEDIUM risk from terrorist attack must have a Counter-Terrorist contingency plan in place. This must seek to deter or minimise impact of an attack or hostile interest and must include:

a) Details of all protective security measures (including physical, personnel, information) to be implemented following an increase, or decrease, in the Government Response Level.

b) Instructions on how to respond to a specific threat, event or item (e.g. telephone bomb threat, a suspicious package or delivery, Vehicle Borne Improvised Explosive Device (VBIED), hostile reconnaissance or hostile individuals).

c) A search plan.

d) Evacuations plans, including details on securing premises in the event of full evacuation.

e) Business continuity plans.

f) A communications and media strategy, including handling enquiries from concerned family and friends.

g) Liaison with emergency services and any multi-agency contingency plans.

Government establishments that are assessed to be at LOW threat from terrorist attack must ensure that these requirements are incorporated into general business continuity plans (see MR 70)

Protective security measures

12. This framework provides detailed policy and guidance on all aspects of protective security and DSOs must refer to these when developing CT policies and plans, but in broad terms they need to ensure:

a. **Physical security -** That establishments (both new construction and existing), including non- government establishments which sustain HMG business, such as data centres, are suitably robust and offer an appropriate degree of protection against attack and hostile interest. Considerations may include protected spaces, glazing, stand-off, barriers, CCTV, public areas, internal communications, signage, Perimeter Intrusion Detection systems (PIDs), access points and control, building services (e.g. ventilation inlets) and parking areas.

b. **Personnel security -** There is adequate protection for all staff, as well as personal protection arrangements required for high-threat personnel such as Ministers and VIPs. National Security Vetting is a core element of ensuring trusted individuals are employed in sensitive posts. The Counter-Terrorist Check (CTC) plays an important part in CT vetting measures but other aspects of personnel security must be considered equally important, such as the Baseline Personnel Security Standard (BPSS) and ongoing personnel security management.

c. **Information security -** That all ICT systems, as part of the formal ICT accreditation process, consider and mitigate potential physical and electronic terrorist attack, and that CT plans include the need to protect electronic and paper based information from unauthorised access, compromise or destruction.

Testing CT arrangements

13. Testing and exercises are essential elements in providing assurance – they ensure that staff are well versed in procedure, that equipment and communications are functioning and adequate and that arrangements with external bodies (e.g. emergency services, contractors, suppliers) are effective. They also provide an opportunity to identify and address problem areas. The testing of CT arrangements should form an important part of testing overall Business Continuity and emergency response plans.

MANDATORY REQUIREMENT 68

As part of Business Continuity and emergency response plans, Departments and Agencies must test their Counter-Terrorist contingency plans regularly to ensure that plans are effective and that any potential problems are identifies and remedied. Minimum requirements are:

a) HIGH risk - at least annually

b) MODERATE risk – at least once every two years

c) LOW risk – at the least every 3-5 years or part of broader business continuity and emergency evacuation tests.

Assurance

MANDATORY REQUIREMENT 69

Departments and Agencies must:

a) Submit a brief report to the Head of Department summarising the additional protective measures implemented following any increase in the Government Response Level;

b) Provide an explicit statement of assurance on Counter-Terrorist protective security as part of the annual security report made by the DSO to their Head of Department (MR6)

c) Report the results of any tests of Counter-Terrorist protective security plans in the annual security report to the Head of Department.

Security Policy No.7: Business Continuity

1. This is the seventh Security Policy within the HMG Security Policy Framework (SPF); outlining the mandatory security requirements and management arrangements to which all Departments and their Agencies (defined as including all bodies directly responsible to them) **must** adhere.

What is Business Continuity Management?

2. The British Standard on Business Continuity Management (BCM), BS 25999 defines BCM as a: 'holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities'.

3. Business Continuity Management (BCM) is the process through which Departments aim to continue their critical business activities following a disruption and effective recovery afterwards (return to 'normal'). It is an essential aspect of securing their business.

MANDATORY REQUIREMENT 70
Departments and Agencies must have robust, up to date, fit for purpose and flexible business continuity management arrangements that are supported by competent staff that allow them to maintain, or as soon as possible resume provision of, key products and services in the event of disruption. These arrangements must follow industry best practice (BS25999 or equivalent standard) and Departments and Agencies must be able to clearly evidence alignment to this level.
BCM arrangements must be tested and reviewed at least annually or following significant organisational change.

What should a BCM system look like?

4. An effective BCM programme will have the following features:

- A BCM strategy endorsed and supported by Board level management.
- A BCM programme appropriate to the size and complexity of the department.
- Planning to proportionately manage the impact of events and recover from them.
- BCM arrangements that are exercised, reviewed and renewed as appropriate for the organisation and supported by adequately trained staff.
- Communications that ensure that all staff are aware of the BCM arrangements and of their responsibilities within them.

What are the outcomes of a BCM programme?

5. The outcomes of an effective BCM programme are that:

- Key assets, products and services are identified and protected, ensuring their continuity.
- An incident management capability is developed to provide an effective response.
- The organisation's understanding of itself and its relationships with other departments and organisations to include Local Authorities and the Emergency Services is properly developed, documented and understood.
- Staff are trained to respond effectively to an incident or disruption.
- Stakeholder requirements are understood and able to be met.
- Staff and stakeholders receive adequate support and communications in the event of a disruption.
- The organisation's supply chain is secured.
- The organisation's reputation is protected.

6. Strong Business Continuity Management in Government Departments provides leadership to other public and private sector organisations; sending a message of reassurance to citizens and business, and demonstrating to international partners that the United Kingdom is a secure place to trade.

The British Standard for Business Continuity Management: BS 25999

7. BS 25999 provides a basis for understanding, developing and implementing Business Continuity within an organisation. The standard comprises two parts:

- Part 1, the Code of Practice, provides BCM good practice recommendations.
- Part 2, the Specification, provides the requirements for a Business Continuity Management System (BCMS) based on BCM good practice and can be used to demonstrate compliance via an auditing and certification process.

8. It is recommended that Departments and Agencies work towards aligning their Business Continuity arrangements with BS 25999.

VERSION HISTORY

SPF VERSION	DATE PUBLISHED	SUMMARY OF CHANGES
V.1.0	DEC 08	N/A
V.2.0	1 MAY 09	Version History inserted. No other changes to Tier 1-3 text.
V.3.0	OCT 09	N/A
V.4.0	May 10	Mandatory Requirements 10 and 17 were merged; MR 17 is no longer in use. MR 13 – the text has been retained but is no longer considered appropriate as a Mandatory Requirement for all Departments and Agencies. MR 51 has been clarified. MR 66-69 has been amended to introduce more flexibility for Departments and Agencies. MR 70 has been revised to make the requirement more specific. Security Policy No.1 – New paragraph (15) added covering international exchanges Security Policy No.2 – Para 13 replaced with new para (14) cross referencing Security Policy No.1 (MR10) Security Policy No. 3 – Para 12 & 13 – minor changes for clarity Security Policy No. 4 – New para (2) inserted reflecting the importance of cyber space and associated security challenges. Para 11 – newly inserted concerning the role and functions of the Cyber Security Operations Centre (CSOC) Security Policy No. 5 – General clarity throughout policy section.

		Security Policy No. 6 - Para 2 – Web link updated MR 68 and 69 have been swapped round. Security Policy No. 7 – MR expanded to clarify BCM requirements and alignment with BS25999

CONTACT DETAILS

The Cabinet Office is responsible for developing and communicating the Security Policy Framework.

E-mail : SPF@cabinet-office.x.gsi.gov.uk.

Publication date: May 2010