Cabinet Office

HMG Security Policy Framework

Version 8 – April 2012

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 Departments. Ultimately, however, security is the responsibility of everyone and our policies and processes will only work well if we all play our part.

The Security Policy Framework describes the principles and approaches that Government applies to protect its assets, be they people, infrastructure or information, whilst at the same time assisting in the delivery of public services. This edition has been significantly revised to join up and simplify policy, eliminate unnecessary red tape and clarify the key security outcomes that we expect Departments and Agencies to achieve through robust, impact driven risk management approaches; always informed by a clear understanding of the threat and the needs of the business.

The framework is an integral part of our broader agenda to modernise and transform Government and public services. The ever-increasing pace of change offers great opportunities as well as some security challenges. This policy framework provides a common structure for Departments to work together to manage these challenges, as well as seeking out opportunities to share security functions and capabilities, and to foster a positive and professional culture of security across the government estate.

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:

1. This Security Policy Framework (SPF) describes the security controls to be applied to UK Government assets. It focuses on security outcomes that are necessary to achieve a proportionate and risk managed approach to security that enables government business to function effectively, safely and securely.

Government Security Responsibilities

2. The Prime Minister and Cabinet are ultimately responsible for the security of Government. Practical responsibility is delegated to the Cabinet Secretary, exercised through his role as Chairman of the Official Committee on Security (SO). Within Departments and Agencies, accountability for security arrangements rests with Ministers, Permanent Secretaries (Heads of Departments) and their respective Management Boards. A network of Departmental Security Officers (DSOs), manage day to day security arrangements, working to the corporate standards set out in this framework and risk assessments as agreed by the Accounting Officer / Head of Department and Management Board.

3. The Cabinet Office is responsible for protective security policy and promulgates this across government. Departments and Agencies are responsible for protecting their assets – information, personnel and physical – according to these policies and as appropriate to their business needs and circumstance. Departments and Agencies are best placed to assess the risks they face, and must develop their own security policies in line with this framework.

4. This Security Policy Framework (SPF) comprises mandatory security considerations that all Departments and Agencies must address, and security outcomes that should be achieved. It also describes assurance and compliance arrangements that organisations must apply. The SPF cannot simply be applied as departmental security policy; it must be used, adapted and applied to meet the specific business needs of the organisation and its delivery partners. It sets the minimum standard, but some organisations may need to apply enhanced security controls, appropriate to their circumstances and in line with the risk appetite determined by their Ministers, Permanent Secretary / Head of Department and Management Board.

5. The SPF should also be extended, as appropriate, to organisations or suppliers working on behalf of government, handling HMG assets or delivering services including: Non-Departmental Public Bodies (NDPBs), contractors, Emergency Services, devolved administrations, Local Authorities, or any regular suppliers of goods and / or services. This includes those with responsibility for delivering shared services (both private and public). 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 suppliers, where equivalent security policies are acceptable and the level of oversight needed to assure themselves that assets are properly protected. This policy is supplemented by detailed advice and guidance which the DSO can tailor to their particular requirements and distribute on a 'need to know' basis.

Role of the Centre

6. 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 (GSS) provides the secretariat for SO and is responsible for developing and communicating this framework, supporting Departments and Agencies to ensure an appropriate degree of compliance with the minimum requirements by sharing best practice and encouraging consistency and shared capabilities. The GSS works closely with the national technical authorities:

Centre for the Protection of National Infrastructure (CPNI)

6.1 CPNI provides integrated security advice (combining information, personnel and physical) to organisations which make up the national infrastructure, to reduce the vulnerability of the national infrastructure (primarily the critical national infrastructure) to terrorism and other threats to national security.

CESG

6.2 CESG is the UK National Technical Authority for Information Assurance. Its objective is to protect and promote the vital interests of the UK by providing advice and assistance on the security of communications and electronic data. CESG deliver information assurance policy, services and advice that government and other customers need to protect vital information services.

UK National Authority for Counter-Eavesdropping (UKNACE)

6.3 UKNACE provides expert advice to government on the technical means to detect or prevent eavesdropping devices compromising the security of a site.

And with other partners, including:

Office for Cyber Security and Information Assurance (OCSIA)

6.4 OCSIA supports the Minister for the Cabinet Office and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates departments and agencies in driving forward the UK government's cyber security programme to provide the UK with the balance of advantage in cyberspace.

Cyber Security Operations Centre (CSOC)

6.5 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 main 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. CSOC is accountable to OCSIA within Cabinet Office.

Civil Contingencies Secretariat (CCS)

6.6 CCS is the Cabinet Office secretariat responsible for enhancing the UK's capability to prepare for, respond to and recover from emergencies. CCS co-ordinate stakeholders across central government and the Devolved Administrations, and work closely with the local responders to improve resilience and ensure that Government can continue to function and deliver public services during a crisis. They also provide information for individuals and businesses to support the building of community and corporate resilience.

Head of Profession for Government Protective Security

6.7 GSS is also supported by a Head of Profession for Protective Security who sponsors efforts to drive professional standards across the government security community and works with GSS to ensure that security policy meets DSO requirements and is both practical and proportionate for the business.

Policy Context

7. Protective security is a corporate service that enables the secure and efficient conduct of individual government departments' business and services. But it also contributes to wider national security strategic objectives, including the protection of our national infrastructure and cyber space:

National Security Strategy (NSS)

7.1 The National Security Strategy ('A Strong Britain in an Age of Uncertainty', Oct 2010) describes Britain's role in the world, the risks to our security and their implication for the UK. It highlights four strategic national security priorities: counter terrorism, cyber security, international military crisis and national disasters such as floods and pandemics.

Strategic Defence and Security Review (SDSR)

7.2 The Strategic Defence and Security Review (*'Security Britain in an Age of Uncertainty',* Oct 2010) assesses the UK's defence, security, intelligence, resilience, development and foreign affairs capabilities in the round, and sets out the ways and means by which to achieve the ends set out in the National Security Strategy.

CONTEST

7.3 CONTEST is the government's long-term strategy for reducing the risk to the UK and its overseas interests from international terrorism. It was published in July 2006 and updated in July 2011; details can be found on the Home Office website. The CONTEST programme is organised into four strands that together deliver a coherent and integrated approach to reducing the vulnerability of the UK to terrorism:

- Prevent – countering the radicalisation of individuals;
- Pursue – investigating and disrupting terrorist activity at home and abroad;
- Protect – reducing the vulnerability of the UK to terrorist attack;
- Prepare – where an attack cannot be stopped, to mitigate its impact.

UK Cyber Security Strategy

7.4 The Cyber Security Strategy provides the overarching context for the transformative national Cyber Security Programme announced in the Strategic Defence & Security Review, closing the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyberspace. It is available on the Cabinet Office website and sets out how the Government will use, influence and act in cyberspace to:

- Create a security foundation for the UK's continued economic prosperity;
- Secure the UK's National Security Interests;
- Protect and promote the UK's way of life.

Civil Contingencies

7.5 The Civil Contingencies Act (2004) provides a single framework for civil protection in the UK. Part One focuses on local arrangements, establishing statutory roles and responsibilities for local responders (including a duty to share information). Part Two focuses on emergency powers, creating a framework for the use of special legislative measures that might be necessary to deal with the effects of the most serious emergencies. The Civil Contingencies Secretariat (CCS) co-ordinate the UK Resilience Capabilities Programme to develop a robust infrastructure of response capabilities to deal rapidly, effectively and flexibly with the consequences of civil emergencies. Further details can be found on the Cabinet Office website.

8. Protective security also underpins and enables the Government's broader social and economic policy objectives, particularly the cross-cutting work to reduce government waste, improve accountability, and deliver modernisation and structural reform. The Efficiency and Reform Group (ERG) in Cabinet Office leads work across a range of areas (e.g. ICT, procurement, communications and Civil Services capabilities), and sponsors transformative projects to share capabilities, improve services and delivery savings. This includes:

- The Government ICT Strategy (March 2011); a transformative programme to deliver better public services at less cost. It will fundamentally change how government incorporates ICT into its everyday business, from the early factoring of technology considerations into the design of policy, reducing operational costs, ensuring information is shared and transparent where possible and always handled appropriately and supporting our plans for economic growth, to enabling workforce transformation so that we have the tools to deliver modern, effective public services.

- The Transparency agenda, developing a more embedded approach to open data throughout the public sector. This will enable accountability, improve outcomes and productivity in key services through informed comparison, transform social relationships – empowering individuals and communities, and drive dynamic economic growth by enabling re-use of public data in innovative ways.

- Other programmes include HMG Online (moving delivery of Government services to the citizen and business online) Estates Rationalisation, Public Bodies Reform and Greener Government.

Critical National Infrastructure (CNI)

9. The national infrastructure is a complex mix of networks, systems, sites, facilities and businesses that deliver goods and services to citizens, and supports our economy, environment and social well-being. Within the national infrastructure, nine sectors have been identified as providing essential services that are the fundamental services upon which daily life in the UK depends. The nine sectors are: food, energy, water, communications, transport, health, emergency services, government, and finance.

10. Within these nine sectors, the Government has identified certain assets as being of strategic national importance to essential service delivery. These are collectively known as the Critical National Infrastructure (CNI). The loss or compromise of these assets would have a severe, widespread impact on a national scale. CNI Sector Sponsors should encourage their community to apply robust security approaches in line with this framework. Where Government Departments are directly responsible for CNI assets, the security requirements to protect these assets should be agreed in partnership between the Department, the National Technical Authorities and the Cabinet Office.

Legal requirements

11. Protective security may also assist organisations to meet a range of statutory requirements, including the Data Protection Act 1998. However, the SPF is not intended to provide legal guidance. Departments will need to take legal advice on a case by case basis in relation to information law (including on the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004), the Official Secrets Act 1989 and the Regulation of Investigatory Powers Act 2000. Legal advisers within Departments will also be able to assist in relation to employment law and compliance with the Human Rights Act 1998 and the Equality Act 2010. The SPF is not intended to be a substitute for expert legal advice on a case by case basis.

Compliance

12. Compliance arrangements and assurance mechanisms are based around self

assessment, independent challenge and central reporting. Departments and Agencies must assure themselves that security arrangements in their core organisation and wider family are appropriate and fit for purpose, providing an annual report to their Permanent Secretary / Accounting Officer. They must provide an exception report to Cabinet Office on an annual basis, noting any significant security events or issues. Any control weakness or areas of non-compliance with the SPF will also need to be addressed in the Department's Governance Statement; publicly available as part of the annual Resource Accounts.

13. While the SPF is intended to cover the United Kingdom, responsibility for managing local security arrangements is devolved to the Scottish, Welsh and Northern Irish Devolved Administrations. The Government works closely with these bodies to ensure that sensitive information and other assets are protected to equivalent standards across the UK. Similarly, organisations such as the National Health Service, Police forces and Local Government all handle sensitive government assets and must protect this material appropriately.

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.

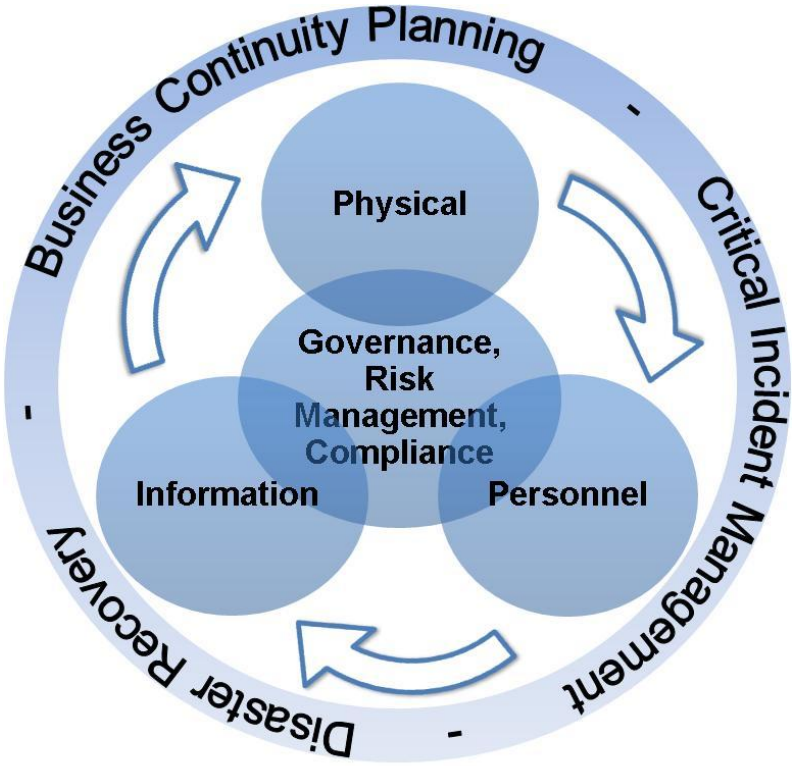
3. Departments and Agencies must be able to share information (including personal data) confidently knowing it is reliable, accessible and protected to agreed standards irrespective of format or transmission mechanism.

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 and Security Approaches

14. Protective security is a risk management process to protect assets (i.e. people, information, infrastructure and facilities) and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. Physical, technical and procedural controls need to be balanced to achieve an appropriate security approach that meets the needs and circumstances of an organisation. These controls should be supported by effective and resilient business processes to respond to, investigate and recover from any incidents:



Roles, accountability and responsibilities

15. The Head of Department / Permanent Secretary is responsible and ultimately accountable for security within their organisation. They must determine appropriate security structures for their core organisation and any organisations for which they are responsible.

MANDATORY REQUIREMENT 1

Departments and Agencies must establish an appropriate security organisation (suitably

staffed and trained) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.

To comply with this requirement, Departments and Agencies must:

- Appoint a Board-level representative for Security (e.g. Head of Department / Permanent Secretary);
- Appoint a designated Senior Information Risk Owner (SIRO) responsible for managing the organisation's information risks, including maintaining an information risk register;
- Appoint a designated Departmental Security Officer (DSO), with day-to-day responsibilities for all aspects of Protective Security;
- Consider the need for other specialist security roles, including a Lead Accreditor, IT Security Officer (ITSO), Communications Security Officer (COMSO), and Information Asset Owners. Organisations may combine roles or else pool security resources with other similar-sized bodies;
- Clearly set out where security responsibilities lie, including the relationship between the Department's main Board and the Boards of their Agencies or other bodies;
- Ensure that all individuals with designated security responsibilities (including DSU staff) undertake appropriate training for their role.

16. Where Departments or Agencies utilise shared services or assets, responsibilities for the risk management of those shared services / assets should be agreed and documented.

Security Risk Management

17. Security needs to be approached in a structured and outcome focussed way to ensure that risks are managed appropriately, in line with the following principles:

1. Identify Assets: understand the value of assets (people, information, services etc) how they support the business and the impact of compromise or loss; assign appropriate asset owners, including responsibilities for a shared assets or services;
2. Assess Threats: identify the threats to the organisation's assets, and assess the scale of the threat (in terms of motivation, capability and opportunity) and impact of a threat occurring;

3. Assess Vulnerabilities: consider the vulnerability of assets, systems and services to compromise, including an assessment of the adequacy of existing safeguards;
4. Risk Tolerance: understand the level of risk that the organisation is prepared to tolerate in order to achieve their business aims;
5. Implement Controls: select proportionate security controls as necessary to reduce the risk to an acceptable level. Risks should be continuously monitored and corrective action taken where necessary.

18. The level of acceptable risk should be agreed by the organisation's Management Board and kept under review. It will vary from organisation to organisation and in some cases may exceed the minimum requirements set out in this framework. **Risk avoidance is not risk management:** the approach taken must be both transparent and justifiable.

19. Security risks should be regularly reviewed and re-evaluated, and risk management principles embedded as part of day-to-day business. Departmental approaches must be flexible and capable of adapting to fast moving or unpredictable events that require dynamic decision-making.

MANDATORY REQUIREMENT 2

Departments and Agencies must:

* Adopt a holistic risk management approach covering all areas of protective security across their organisation.
* Develop their own security policies, tailoring the standards and guidelines set out in this framework to the particular business needs, threat profile and risk appetite of their organisation and its delivery partners.

To comply with this requirement, Departments and Agencies must:

- Apply the principles and concepts set out in the HM Treasury Orange Book on Risk Management, informed by Planning Assumptions derived from the National Risk Register, to help determine a level of risk appetite that is appropriate to their organisation's circumstances, business and threat profile;
- Apply the risk assessment methodologies mandated throughout this framework as part of an holistic risk management approach;
- Maintain a detailed Risk Register (with assigned risk owners) recording any specific vulnerabilities or security risks, the control measures taken to mitigate these risks,

and any adjustments over time following changes to the threat environment. Subject to security considerations, the risk register should be made widely available within the organisation to ensure all business units have an input.

Departmental CNI Assets

20. Departments and Agencies must identify any systems, facilities or business services that they manage that are of strategic national importance in terms of the delivery of essential public services, the maintenance of the UK's economic prosperity and social well-being, or the continuity of government and national defence. The loss or compromise of such assets would have a severe, widespread impact on a national scale and Departments must work with the National Technical Authorities and the Cabinet Office to ensure they are afforded appropriate levels of protection.

Culture, education and awareness

21. 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. Departments and Agencies must ensure that all staff are briefed on their security responsibilities on induction and have access to regular refresher training, awareness programmes and security briefings. These should cover individual 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 counselling and support services or to an independent arbiter.

22. Departmental security policies must be widely available internally and referenced in overall business plans. Policies on security breaches, information management, ICT system operating procedures and access control polices must be made available to all staff and staff must be specifically briefed on their personal responsibilities and the potential consequences of breaching security rules.

MANDATORY REQUIREMENT 3

Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.

To comply with this requirement, Departments and Agencies must ensure that:

- All staff are provided with simple, plain English guidance with regards to the Official Secrets Acts, Data Protection Act and the Freedom of Information Act. Staff handling protectively marked information must be given specific guidance on how this legislation relates to their role;
- Security education and awareness is built in to all staff inductions, with regular familiarisation thereafter. All staff should be aware of the department's security breach policy and understand the potential sanctions for inappropriate behaviours (whether accidental or deliberate). Departmental breach policy must be consistent with Human Resources policy and employment law;
- 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;
- There is a clearly stated and available policy, and mechanisms in place, to allow for independent and anonymous reporting of security incidents.

23. Staff that have privileged access to key departmental assets (e.g. ICT system administrators) should be given enhanced training about their responsibilities and be aware that inappropriate behaviours may lead to disciplinary or criminal proceedings.

Delivery Partners and Suppliers

24. Departments and Agencies are increasingly outsourcing the provision of ICT systems and business and information services through a network of public sector delivery partners and commercial suppliers and shared services. These organisations represent key areas of risk and Departments and Agencies must ensure that appropriate security controls are in place to reduce the risks to an acceptable level, along with effective governance controls to monitor compliance and respond to incidents.

Managing and Recovering from Incidents

25. Departments and Agencies manage a variety of sensitive assets and essential public services that are vital to assure the health, safety, security and economic well-being of the nation, and the effective functioning of government. They must put in place appropriate

policies and procedures to mitigate a range of potential security incidents and ensure that critical business activities can be quickly resumed following a disruption. This could include:

- Physical security Incidents – resulting from either criminality (e.g. forced break-in, terrorist attack etc) or other hazards (e.g. flooding);
- Information breaches – compromise or loss of information through carelessness, theft, insider fraud, deliberate leaking or malicious attack (i.e. espionage); or,
- Cyber / ICT security incidents – resulting from electronic attacks, compromise of communications security or disruption of online services.

MANDATORY REQUIREMENT 4

Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.

To comply with this requirement, Departments and Agencies must:

- Ensure they have put in place an effective and up-to-date Business Continuity Management (BCM) system to enable them to maintain or else quickly resume provision of key services in the event of a disruption. BCM arrangements must follow industry best practice (BS25999 or equivalent standard) and Departments and Agencies must be able to clearly evidence alignment to this level. This must include disaster recovery plans for key ICT systems, along with appropriate arrangements to minimise the impact of a terrorist attack or other critical incidents;
- Ensure that organisation's BCM strategy is endorsed by Board-level management, regularly exercised and reviewed, and supported by competent and well trained staff;
- Put in place effective systems for detecting, reporting and responding to security breaches, including appropriate management structures, investigation capabilities and escalation procedures;
- Adopt the specific incident management methodologies mandated throughout this framework as part of an holistic approach, including developing and testing an incident management plan and promptly reporting any incidents to the relevant government authority.

26. The specific management processes, response arrangements and reporting channels will depend on the type of incident and are described within the respective SPF security discipline (Personnel, Information or Physical).

Assurance and Reporting

27. Self-assessment by Departments and Agencies, central reporting to the Cabinet Office and Parliamentary oversight together combine to provide a robust level of assurance that security and information risks are appropriately managed across government:

- *Self Assessment:* Departments and Agencies are responsible for carrying out internal reviews (at least annually) of protective security and the management of information risks across their organisation, including any delivery partners and / or suppliers with whom they exchange information to deliver services on their behalf. An Annual Report must be submitted to the Accounting Officer / Head of Department for discussion with the Management Board and further action as necessary.

- *Central Reporting:* Departments and Agencies are required to submit an annual Security Risk Management Overview (SRMO) to the Cabinet Office (GSS) indicating any key areas of concern or non-compliance with SPF Mandatory Requirements. An element of independent challenge should be applied in whole or in part to this process. The GSS uses SRMO returns to inform the development of policy and will report significant issues to the Official Committee on Security as necessary.

- *Parliamentary Oversight:* The Accounting Officer / Head of Department is responsible for including any significant security control weaknesses in the Governance Statement, submitted to Parliament as part of the annual Resource Accounts.

MANDATORY REQUIREMENT 5

Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.

To comply with this requirement, Departments and Agencies must:

- Have a system in place to provide assurance that their organisation (and any delivery partners and 3rd party suppliers) comply with relevant security policy requirements. Independent challenge is an important part of this process;

- Produce an annual report to their Head of Department on the state of all aspects of protective security and information risk, including an explicit statement of assurance on Counter-Terrorist protective security;
- Report to the Head of Department about additional protective measures implemented following any increase in the Government Response Level, and any tests;
- Reflect any significant control weaknesses in the Governance Statement to the annual Resource Accounts;
- Submit or contribute to an annual Cabinet Office Security Risk Management Overview.

Security Policy No.2: Security of Information

Introduction:

28. Information is a key asset to Government and its correct handling is vital to the safe and effective delivery of public services. Departments and Agencies need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed, whether managed within the organisation or by delivery partners and suppliers. Equally, Government has a legal obligation and duty to safeguard personal data entrusted to it by citizens and businesses. In striking the right balance between enabling public services and sharing and protecting data, organisations must assess and manage the risks to the services they provide and to the Confidentiality, Integrity and Availability (C, I & A) of the information assets they are formally responsible for.

29. As the UK's 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 to Government information and services range from hostile states and terrorists, to criminals and low level hackers. The way the government views and approaches information security must be cognisant of this dynamic and pervasive cyber environment. Departments and Agencies should also continue to guard against potential threats to their information assets originating from within their own organisations whether malicious or unintentional.

Information Security Management Principles

30. Information Security describes the application of control measures to protect the confidentiality, availability and integrity of systems and services; Information Assurance (IA) describes the steps taken to gain confidence that these controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. The International Standard for Information Security Management Systems (ISO/IEC 27001) is acknowledged as good practice and this policy is aligned to the principles contained in the standard.

31. Information risk should be managed according to the broad principles outlined in 'Security Policy No. 1: 'Governance and Security Approaches', and control measures must complement wider approaches to transparency and knowledge management. The following process describes the application of those principles to the management of information risk:

- Understand the business services and functions that information and information services (including online transactional services) support, including the level of risk that the organisation is prepared to tolerate in order to achieve its business aims;
- Identify information assets (including sensitive or business critical information or services, and any personal / customer data) and value them in terms of the impact from loss of confidentiality, integrity and availability;
- Evaluate the range of threat sources and actors that are relevant and the level of threat they present to the service and information assets;
- Assess the scale of any risks, including an understanding of any vulnerabilities;
- Manage risks proportionately through application of an appropriate mix of technical, procedural, personnel and physical controls and assign an appropriate level of protection to mitigate, and / or recover from, the potential loss or failure of those assets;
- Continuously review information risks, monitor the effectiveness of security controls and take corrective action as needed.

Information Security Policy

MANDATORY REQUIREMENT 6

Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.

To comply with this requirement, Departments and Agencies must:

- Identify and assign information security roles and responsibilities appropriate to the size, structure and business function of their organisation
- Adopt policies, procedures and controls to ensure information assets are identified, valued, handled, stored, processed, transmitted, shared and destroyed in accordance with legal requirements and in line with the standards set out in the Government Protective Marking System (GPMS) and the supporting CESG technical and IA Standards;
- Ensure that any information received from foreign governments or international organisations (such as NATO and the EU), including their authorised contractors, is

handled and protected in accordance with relevant international security agreements; where no such agreement is in place foreign classified information must be protected to the same standard as equivalent UK information;

- Manage the risks associated with digital continuity and records management in respect of all data held electronically, particularly in the event of upgrades in technology, transferral of data into archives and the overall life cycle of data;
- Assess any security and business risks before deciding to outsource or offshore information and/or services. Data or services that relate to or directly support national security should not normally be off shored.

Valuing and Classifying Assets

32. The Government Protective Marking System (GPMS) is the Government's administrative system to ensure that access to information and other assets is correctly managed and that assets are safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, processing, storage, transmission and destruction. The system is designed to support HMG business, and meet the requirements of relevant legislation, international standards and international agreements. It is designed to protect information (and other assets) from accidental or deliberate compromise, which may lead to damage and/or criminal offence; it must therefore be viewed against the legal background including the requirements of the Official Secrets Acts (OSA, 1911 and 1989), the Freedom of Information Act (2000) and the Data Protection Act (DPA, 1998).

33. The Protective Marking System comprises five markings (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT) indicating in descending order the likely impact resulting from compromise or loss. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed. Markings can be applied to any government asset, although they are most commonly applied to information held electronically or in paper documents. With respect to information and communication systems, the likely damage (i.e. compromise of confidentiality, availability or integrity) is expressed in terms of Business Impact Levels.

34. Access to sensitive information or assets must only be granted to those who have a business need and the appropriate personnel security control (Baseline Personnel Security

Standard (BPSS) or National Security Vetting (NSV)). 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 7

Departments and Agencies must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in the Government Protective Marking System (including any special handling arrangements) and the associated technical guidance supporting this framework.

To comply with this requirement, Departments and Agencies must ensure that:

- Information and other assets are valued according to the definitions in Annex One and are clearly and conspicuously marked. Where this is impractical (e.g. a building or physical asset) staff must be made aware of the protective controls required;
- Assets are protected in line with GPMS requirements throughout their lifecycle from creation to destruction to ensure a proportionate level of protection against the real and/or anticipated threats faced by such assets;
- Access to sensitive assets is only granted on the basis of a genuine need to know and an appropriate level of personnel security control;
- Where information is shared for business purposes departments and agencies must ensure the receiving party understands the obligations and protects the assets appropriately;
- Assets sent overseas are protected by appropriate national prefixes, caveats and / or special handling instructions. Assets received from overseas nations or international organisations must be protected in accordance with treaty obligations or afforded the same protection as equivalent UK material if no formal agreement is in place;
- All staff handling sensitive government assets are briefed about how legislation (particularly the OSA, FOIA and DPA) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies. Appropriate management structures must be in place to ensure the proper handling, control and (if appropriate) managed disclosure of sensitive assets.

Applying the Correct Protective Marking

35. 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;
- Files or groups of documents must be protected to the standard required for the highest marked document contained within it;
- Compromise of aggregated or accumulated information of the same protective marking is likely to have a higher impact (particularly personal data). This should not generally result in a higher marking but may require additional handling arrangements. If the accumulation of data results in a more sensitive asset being created, then a higher protective marking should be considered;
- The originator or nominated owner of an asset is responsible for applying the correct marking. Sensitivity may change over time and it may be necessary to reclassify assets, or to disclose information under statutory schemes. Any change requires the agreement of the originator or designated owner.

36. Supplementary markings (e.g. national caveats, descriptors, code words etc.) may be applied to protectively marked material to indicate additional information about its contents, sensitivity and handling requirements.

37. Outside of the government sector there is no agreed system for marking sensitive material. Any material originating outside of government that is not covered by a recognised protective marking, but is marked to indicate sensitivity, must be handled and protected to at least the level offered by the PROTECT marking.

Business Impact Levels

38. With regard to ICT systems, Departments and Agencies must use 'Business Impact Levels', also known simply as Impact Levels (ILs), to assess the level of impact likely to result from compromise of Confidentiality, Integrity and Availability. ILs provide a seven-point scale (IL 0 - no impact, to IL6) to help organisations make a balanced assessment of the controls needed to risk manage (potentially differing) confidentiality, integrity and availability requirements. Such decisions must also include an assessment of relevant threats. Organisations must also consider 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.

Personal data

39. Government must handle, protect and share large amounts of personal data to maximise public service delivery. Departments and Agencies have a legal duty to comply with the data protection principles set out in the Data Protection Act. Further procedural requirements are defined in 'HMG IA Standard No.6 – Protecting Personal Data and Managing Information Risk' to ensure a high level of confidence that personal data is handled correctly.

Risk Assessment and Accreditation of ICT systems

40. Risk assessment and accreditation processes provide important assurance that an organisation can accept the balance between business opportunity, risk and cost for any given information system. Designated Accreditors are responsible (on behalf of the Management Board) for ensuring that accreditation processes comply with relevant HMG standards and procedures, and for agreeing any exceptions with their Departmental SIRO and IT Security Officer (ITSO) on a risk management basis.

MANDATORY REQUIREMENT 8

All ICT systems that handle, store and process protectively marked information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Government Secure Intranet, GSI), must undergo a formal risk assessment to identify and understand relevant technical risks; and must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.

To comply with this requirement, Departments and Agencies must:

- Conduct technical risk assessments for all ICT systems or services (using 'HMG IA Standard No. 1 - Technical Risk Assessment'), repeating the assessment annually or whenever there are significant changes to a risk component (threat, vulnerability, business use, impact etc);
- Apply a proportionate selection of technical, procedural, personnel and physical security controls to manage the identified risks to a level that the business can tolerate;

- Record relevant information, the accreditation status and any risk management decisions in a Risk Management and Accreditation Documentation Set (RMADS) using 'HMG IA Standard No. 2 - Risk Management & Accreditation of ICT Systems & Services';
- Comply with specific requirements for the protection and handling of personal data as set out in 'HMG IA Standard No.6 – Protecting Personal Data and Managing Information Risk';
- Have the ability to regularly audit information assets and ICT systems to check compliance and extract data in the event of an incident;
- Where shared systems or services are used, the Department or Agency must satisfy themselves that the use of these systems or services can be managed within its own risk appetite.

Risk Treatment – Technical, Procedural and Physical Security Controls

41. The following technical, procedural and physical security controls should be considered as part of the process of treating the risks identified during an IS1 risk assessment review:

Technical Controls:

MANDATORY REQUIREMENT 9

Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

To comply with this requirement, Departments and Agencies must:

- Comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories (e.g. Government Secure Intranet);
- Put in place a proportionate risk based suite of technical policies and controls including:
    I. Timely Patching against known vulnerabilities; Managing the risks posed by all forms of malicious software ('malware'), including viruses, spyware and phishing etc;

II. Boundary protection (e.g. firewalls) on all systems with a connection to untrusted networks, such as the Internet;
III. Content checking/blocking policies;
IV. Protective Monitoring;
V. Lockdown policy to restrict unnecessary services;
VI. User account management to ensure individual accountability and that no user has more privileges (access and functionality) than required.

- Ensure that they take action to develop and keep up to date an appropriate understanding of new, emerging and changing threats and vulnerabilities;
- Comply with the requirements of 'HMG IA Standard No.4 - Communications Security and Cryptography' for the protection of any cryptographic items. Organisations that handle CESG approved cryptographic material must appoint a Communications Security Officer (ComSo);
- Where applicable, comply with mandated Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations;
- Ensure that all portable devices and media used for mobile or remote working (e.g. laptops, PDAs, mobile phones, memory sticks, external drives, MP3s etc) are appropriately secured. Where possible, only approved mobile devices should be used. CESG should be consulted for advice and guidance where this is not possible;
- For online services, keep abreast of and respond to changing threat conditions. Consider transactional monitoring, especially if these services are value bearing;
- Have 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;
- Ensure that all media used for storing or processing protectively marked information must be disposed of or sanitised in accordance with 'HMG IA Standard No 5 - Secure Sanitisation'.

Procedural Measures:

MANDATORY REQUIREMENT 10

Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.

To comply with this requirement Departments and Agencies must:

- Implement appropriate identification and authentication controls, policies and procedures to manage the risk of unauthorised access, ensure the correct management of user accounts and enable auditing;
- Ensure that ICT users with higher levels of privilege and/or potentially wide access (e.g. system administrators, architects, programmers), or those with responsibilities for ICT security are evaluated for National Security clearances as appropriate;
- Ensure that all users of ICT systems comply with the security operating procedures governing their use, receive appropriate security training, and are aware of local processes for reporting issues of security concern;
- Put in place appropriate policies and procedures to support mobile and remote working and ensure users are briefed on, and accept, their security responsibilities.

Physical Security and Resilience

42. Departments and Agencies must implement proportionate physical security controls to prevent unauthorised access to locations where paper based assets and ICT systems components (including cryptographic items) are stored, including well tested and resilient procedures to ensure critical business or services can be resumed following any disruption. Physical security controls are described in 'Security Policy No.4: Physical Security and Counter-Terrorism; policies and procedures to enable organisations to manage and recover from security incidents (including Business Continuity planning) are set out in 'Security Policy No.1: Governance and Security Approaches'.

Delivery Partners and Third Party Suppliers

43. Departments manage security arrangements within their government delivery chains (delivery partners and third party suppliers) in different ways, proportionate to local business requirements and the level of risk. The SPF and HMG IA Standard No.6 require departments to assure themselves that the organisations within their delivery chain have considered the range of risks to government information and put in place appropriate security controls to reduce the risks to an acceptable level. Where these services involve the management or production of information classified CONFIDENTIAL or above, the site (or area) where this material is held or processed must be accredited to List X standards. The respective third party supplier must also put in place effective governance controls to monitor compliance and respond to (and report) any incidents. In all cases the Department remains responsible for their information risks, even where services or system delivery is entirely outsourced.

MANDATORY REQUIREMENT 11

Departments and Agencies must ensure that the security arrangements among their wider family of delivery partners and third party suppliers are appropriate to the information concerned and the level of risk to the parent organisation. This must include appropriate governance and management arrangements to manage risk, monitor compliance and respond effectively to any incidents.

Any site where third party suppliers manage assets at CONFIDENTIAL or above must be accredited to List X standards.

To comply with this requirement, Departments and Agencies must:

- Seek assurance from their delivery partners that they are managing their protective security and information risks to an appropriate level;
- Work closely with security, procurement and contract management teams to ensure that adequate security, information assurance and business continuity requirements are specified in contracts with third party suppliers, and that all contracts involving the handling of personal data adhere to the Office of Government Commerce (OGC) model terms and conditions;
- Comply with HMG requirements and procedures governing the off-shoring of data;
- Put in place appropriate governance arrangements to annually review the compliance of delivery partners and third party suppliers against the requirements of this framework. The management of assurance activities must be independent of the organisation providing the service.

Shared Services

44. The principles and requirements of this Framework remain applicable when two or more government organisations share a service. When entering into shared services arrangements or deciding to participate in an existing service, Departments and Agencies must ensure that the shared service is appropriate for their individual business needs and risk appetite. As a matter of course the DSO and / or ITSO should be consulted before entering into a shared service arrangement.

45. It is appropriate to re-use shared service risk assessments, assurance and approval processes, but each participating Department or Agency retains ultimate responsibility for managing any risks to their information.

Managing and Reporting Security Incidents

MANDATORY REQUIREMENT 12

Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.

To comply with this requirement, Departments and Agencies must:

- Put in place a security incident policy setting out clear guidance for staff on the potential disciplinary and / or criminal penalties that may result from failure to comply with security policies (including through the deliberate or accidental compromise of protectively marked information), and their responsibilities to report incidents promptly;
- Put in place appropriate and well tested management structures and procedures to co-ordinate the organisation's response to information security incidents and ensure all staff are aware of the procedures for reporting incidents;
- Ensure that sufficient data is collected and available for post incident investigations;
- Ensure incidents are reported to the relevant central authority:
    - HMG incident management bodies: GovCERT for network incidents and CINRAS for communications security incidents involving CESG approved cryptographic items;
    - The Information Commissioner's Office for significant actual or possible losses of personal data, Cabinet Office Government Security Secretariat (GSS) should also be notified;
    - Cabinet Office GSS for any unauthorised leaks of government information;
    - Cabinet Office GSS (as the National Security Authority) for any security incidents concerning classified information received from foreign governments or NATO, the EU or the European Space Agency and their subsidiary organisations.

Security Policy No.3: Personnel Security

Introduction

46. Personnel security is applied to provide assurance as to the trustworthiness, integrity and reliability of HMG employees, contractors and temporary staff. As a minimum requirement, all staff are subject to the recruitment controls described in the Baseline Personnel Security Standard (BPSS). Where access to more sensitive assets is required, National Security Vetting (NSV) may be applied to ensure that such posts are filled by individuals who are unlikely to be susceptible to influence or pressure which might cause them to abuse their position.

Risk Management

47. In keeping with protective security principles generally (described in 'Security Policy No. 1: 'Governance and Security Approaches'), Departments and Agencies must apply a risk management approach to determine the appropriate levels of personnel security controls. These controls cannot provide a guarantee of reliability and must be supported by effective supervision and line management, and be underpinned by proper application of the "need to know" principle, access and information security controls.

Recruitment Checks and National Security Vetting

48. The BPSS is the recognised standard for HMG recruitment checks, and addresses the risks associated with identity fraud, illegal working and deception generally. It comprises four main elements: an identity check, an employment history check, nationality and immigration (including right to work) check, and (where NSV is not required for the post) a check of unspent criminal record. Prospective employees are also required to account for any significant periods spent abroad. An individual who meets the requirement of the BPSS may have access to official assets, including (subject to "need to know") regular access to UK RESTRICTED and UK CONFIDENTIAL, and occasional access to UK SECRET.

49. There are three levels of NSV: the Counter Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). These must only be applied where a risk assessment indicates that it is appropriate and proportionate to do so, in keeping with the HMG

Statement of Vetting Policy. This statement and full details of the BPSS and National Security Vetting are available publicly on the Cabinet Office website.

MANDATORY REQUIREMENT 13

Departments must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and a proportionate and robust personnel security regime that determines what other checks (e.g. national security vetting) and ongoing personnel security controls should be applied.

To comply with this requirement, Departments and Agencies must:

- Ensure that the Baseline Personnel Security Standard (BPSS) is applied to all individuals employed by or contracted to carry out work for any government department. In any instances where this is not possible (e.g. some overseas recruits), the decision to accept the risk should be recorded;
- Determine the need for, and level of, national security vetting clearance required to fulfil the duties of the post based on a thorough risk assessment;
- Apply national security vetting in accordance with the HMG Statement of Vetting Policy, as transparently as any national security considerations allow;
- Record and maintain appropriate decisions.

Ongoing Personnel Security Management

50. Recruitment and national security vetting checks can only provide a snapshot of an individual at a particular time therefore an ongoing personnel security management regime must be established. This will require senior and line management support, awareness and education, and formal periodic reviews of security clearances.

MANDATORY REQUIREMENT 14

Departments and Agencies must have in place an appropriate level of ongoing personnel security management, including formal reviews of national security vetting clearances, and arrangements for vetted staff to report changes in circumstances that might be relevant to their suitability to hold a security clearance.

To comply with this requirement, Departments and Agencies must:

- Keep full and up to date personnel security records on all employees that hold security clearances;
- Ensure that moves or loans do not commence until the receiving organisation has confirmation of the appropriate security clearance and of any caveats that have been applied;
- Ensure that NSV clearances are formally reviewed according to agreed timescales for each level of clearance;
- Ensure than an Annual Security Appraisal Form (SAF) is completed by all DV holders and, in those instances where is applicable, SC and CTC holders;
- Establish a programme of management where risks or vulnerabilities have been identified;
- Ensure that any new information or concerns that may affect the reliability of an individual are reported to the appropriate authorities.

Appeals

51. Existing employees have a right of appeal against a decision to refuse or withdraw a national security vetting clearance. Internal appeals processes should include an ultimate right of appeal to the Head of Department (or equivalent). If the decision is upheld there is a further avenue of 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 subject to national security vetting. Separate arrangements are available to applicants to, and staff and contractors of the Security and Intelligence Agencies via the Investigatory Powers Tribunal (IPT).

MANDATORY REQUIREMENT 15

Departments must make provision for an internal appeals process for existing employees wishing to challenge National Security Vetting decisions and inform Cabinet Office Government Security Secretariat should an individual initiate a legal challenge against a National Security Vetting decision.

To comply with this requirement, Departments and Agencies must:

- Ensure that the reasons for refusing an existing employee a national security vetting clearance are recorded in full and that the individual is informed, subject to national

security considerations, of the reasons for the refusal with reference to the relevant facts;

- Ensure that the employee is informed, fully and clearly, of the mechanisms for internal and external appeal and that any factual information that can be shared is shared with the individual;
- Provide an agreed factual account of any interview proceedings that gave rise to concerns and ensure that third party information provided in confidence, or information supplied by the Security Service, is not shared with the individual;
- Establish a clear policy on redeploying individuals that have been refused a clearance in areas where identified risks can be managed. This policy should also outline dismissal procedures and handling those instances where it is not possible to continue to employ the individual because of security objections.

Security Policy No. 4: Physical Security and Counter Terrorism

Introduction:

52. Government assets must be safeguarded against a range of physical threats, including crime (theft, criminal damage, assaults on staff etc), natural hazards (e.g. flooding), and national security threats such as terrorism and espionage. Departments and Agencies must determine an appropriate security posture for their estate and put in place effective and proportionate security controls to reduce the risks to their assets (people, information and infrastructure) to an acceptable level. This includes ensuring that assets held or managed by delivery partners and third party suppliers are properly protected.

53. Physical security describes a range of controls that are intended to protect individuals from violence; prevent unauthorised access to sites and / or protectively marked material (and other valuable assets); and reduce the risk a range of physical threats and mitigate their impact to a levels that is acceptable to the organisation. Security must be incorporated into the initial stages of planning, selecting, designing or modifying any building or facility, using appropriate methodologies; putting in place integrated and proportionate control measures to prevent, deter, detect and/or delay attempted 'physical attacks', and to trigger an appropriate response.

54. Physical security measures should complement other technical, personnel and procedural controls as part of a 'layered' or 'defence in depth' approach to security that effectively balances prevention, detection, protection and response. For example, perimeter fencing and access control measures may deter an attack because of the difficulties of gaining access; CCTV or intruder alarms 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.

Counter-Terrorism (CT)

55. The UK Government is perceived by many terrorist groups as an attractive and 'legitimate' target. All Departments and Agencies should be considered as potential terrorist targets and must have in place Counter Terrorism (CT) arrangements that are proportionate to the threat and the assets to be protected, along with contingency arrangements to facilitate the quick resumption of vital services (including contracted services) following an attack. The visible level of security is a factor in terrorist targeting and all government

establishments must implement the baseline CT controls set out in supporting guidance to this Security Policy. For some areas (e.g. high risk sites, nuclear assets / materials, and sites forming part of the UK Critical National Infrastructure) CT security requirements will be intentionally more prescriptive.

Security Risk Assessment

MANDATORY REQUIREMENT 16

Departments and Agencies must undertake regular security risk assessments for all sites in their estate and put in place appropriate physical security controls to prevent, detect and respond to security incidents.

To comply with this requirement Departments and Agencies must:

- Manage their physical security risks in accordance with the requirements set out in 'Security Policy No. 1: 'Governance and Security Approaches' (MR2), in line with the organisation's overall risk tolerance;
- Understand the value of their assets, their location and the impact of compromise or loss, both of the assets themselves and any key buildings (particularly CNI sites). It is best practice to include these in an appropriate, regularly reviewed risk register;
- Determine the level of threat to their assets from different sources (terrorism, espionage, criminal activity, protests etc), including considering the vulnerability of sites to the threats and hazards identified in the National Risk Assessment (NRA) or the National Risk Register (NRR);
- Categorise all establishments (HIGH, MODERATE, and LOW) according to the likelihood of being the target of a terrorist attack, or else in close proximity to an attack;
- Undertake regular security risk assessments for all establishments in their estate (and any non-government sites that sustain core business, such as data centres), using the methodologies and approaches set out in the supporting guidance to this Security Policy or, where appropriate, commercial best practice equivalents;
- Ensure that a detailed Operational Requirement is produced to inform any decision about purchasing or deploying a new security system or product.

56. The 'defence in depth' or 'layered' approach to security starts with the protection of the asset itself (e.g. creation, access and storage), then proceeds progressively outwards to

include the building, estate and perimeter of the establishment. The type and mix of physical and procedural controls will vary depending on the organisation's particular circumstances and business requirements, the nature and level of any threats (terrorism, forced break-ins, covert entry, crime etc) and the cost-effectiveness of the controls. The location and layout of each establishment will also need to be considered, including its surrounding environment, sole or shared occupancy and whether public right of entry is an issue. When selecting measures to balance prevention, protection and response, note that where attackers are not deterred, they should be forced to use tools and methods that facilitate detection and delay.

Internal Controls:

57. Internal physical security controls are mainly used for the protection of sensitive or protectively marked assets to reduce the risk of unauthorised access, loss or damage.

MANDATORY REQUIREMENT 17

Departments and Agencies must implement appropriate internal security controls to ensure that critical, sensitive or protectively marked assets are protected against both surreptitious and forced attack, and are only available to those with a genuine 'need to know'. Physical security measures must be proportionate to level of threat, integrated with other protective security controls, and applied on the basis of the 'defence in depth' principle.

To comply with this requirement, Departments and Agencies must:

- Ensure that sensitive or valuable assets (including paper-based assets, ICT hardware and removable media devices) are physically protected to the standards required by the Government Protective Marking System, including through the use of appropriate security furniture, secure areas, barriers and entry controls (in conjunction with sound procedural and personnel security controls);
- Ensure that any security furniture, windows, doors, locks, barriers and entry controls meet appropriate security standards for the protection of sensitive or protectively marked assets, as set out in the supporting guidance to this Security Policy;
- Put in place and enforce appropriate policies to ensure that visitors, cleaners and maintenance workers are escorted at all times in sensitive areas. This requirement may be risk managed where individuals hold an appropriate level of security clearance. Access control and breach management policies must be made available to all staff, and staff must be briefed on their personal responsibilities (e.g. wearing a

pass at all times when on the premises, escorting visitors and searching their work area if required);

- Adopt 'clear desk' and 'clear screen' policies in areas where sensitive assets are handled (particularly in open plan or shared office areas). Where this is not possible, a risk based approach should be adopted to ensure that sensitive material can only be accessed by individuals with a genuine need to know;
- Ensure that computer screens, faxes, printers, combination locks and office areas that are used to display potentially sensitive information (such as walls, notice boards etc) are sited or screened such that they cannot be overlooked by unauthorised individuals, inside or outside the building;
- Carry out compliance checking activities to ensure the effectiveness of physical security control measures.

Building and Perimeter Security

58. This section concerns measures to control access to an establishment and provide an appropriate degree of deterrence and protection against terrorism or other physical attacks. Note that all government organisations have a statutory 'duty of care' to take reasonable steps to protect staff and visitors from harm.

MANDATORY REQUIREMENT 18

Departments and Agencies must put in place appropriate physical security controls to prevent unauthorised access to their estate, reduce the vulnerability of establishments to terrorism or other physical attacks, and facilitate a quick and effective response to security incidents. Selected controls must be proportionate to the level of threat, appropriate to the needs of the business and based on the 'defence in depth' principle.

To comply with this requirement Departments and Agencies must address the following:

- *Perimeter security:* Establish a secure boundary or perimeter through appropriate use of security barriers and entry controls. The security function of the perimeter is to provide a degree of physical, psychological and / or legal deterrence to intrusion, to define an area of responsibility and to allow for quick identification of suspicious individuals or items. Depending on the level of threat, organisations may consider strengthening perimeter security through the use of street furniture to improve stand-off protection, robust fencing, vehicle barriers, Perimeter Intruder Detection Systems

(PIDS), CCTV and security lighting. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter should also be considered.

- *Building fabric:* Ensure that the external fabric of buildings (external walls, windows, doors etc) is suitably robust to provide an appropriate level of blast protection and resistance to forced or surreptitious attack. Considerations to reduce vulnerability may include blast-resistant glazing (or anti shatter film), protected areas for staff, and the installation of window bars, grilles, shutters, security doors etc.

- *Access Control:* Put in place arrangements to control and monitor access to their estate. Frontline staff (security guards, receptionists etc) have a key role but must be supported by appropriate technical and procedural controls, potentially including:
    - Automatic Access Control System (AACS);
    - Pass or ID system;
    - Visitor control and escorting policy;
    - Pass activated doors, turnstiles etc;
    - Entry and exit searching;
    - CCTV;
    - Vehicle Barriers and Vehicle Identification Passes.
  - Buildings containing protectively marked or other valuable assets should have as few entry and exit points as business functions and safety will allow.
  - Have effective plans or procedures in place for dealing with and intercepting unauthorised visitors, intruders or suspicious items. Such plans must include the ability to systematically search and cordon off areas of the establishment if necessary.

- *Manned Guarding:* Consider the use of manned guard forces to deter hostile activity and provide a rapid response to security incidents. Guard duties and the need for, and frequency of, patrols will depend on the level of threat and any other security systems or equipment that might already be in place.

- *Incoming mail and deliveries:* Put in place procedures to screen incoming mail and deliveries for suspicious items; an off-site mail screening facility is recommended. Delivered items (letters, packets and parcels) could potentially contain: explosive or incendiary devices; blades or sharp items; offensive materials; or chemical, biological

or radiological (CBR) materials. Anyone receiving a suspicious delivery is unlikely to know exactly which type it is, so procedures should cater for every eventuality, as far as it reasonable practicable.

Preparing for Critical Incidents

59. Departments and Agencies need to put in place effective arrangements to increase the security posture of their estate in the event of an increased threat, along with appropriate management controls and contingency plans to respond to critical security incidents including terrorist attack, incursions or break-ins. Specific measures are mandated for protection against terrorist attack, particularly for establishments that are assessed as likely terrorist targets (i.e. HIGH or MODERATE risk).

Threat Levels:

60. Threat Levels are designed to give a broad indication of the likelihood of a terrorist attack. The national 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 Home Office website.

61. In order to ensure Departments have current information on the terrorist threat, the Centre for the Protection of National Infrastructure (CPNI) and Cabinet Office Government Security Secretariat (GSS) produce regular threat updates, some of which can only be seen on a 'need to know' basis. If necessary, access to such information can be arranged through Departmental Security Officers (DSOs).

Government Response Level System

62. 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. 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.

63. The supporting guidance to this Security Policy sets out detailed descriptions of Baseline and Incremental security measures that are required at each Response Level. Specific Baseline CT controls are mandated for all Departments to implement on their estate and address physical and procedural measures that are to be applied. Incremental measures are intended to build upon the Baseline measures in response to a developing threat and, if planned for, can generally be introduced at short notice. These measures are to be applied or removed as advised by changes to the Response Level.

64. DSOs are best placed to assess the risks to their organisation and the vulnerabilities of their estate. As such the precise Incremental measures adopted for each individual site and at each Response Level should be determined by the DSO, in consultation with CPNI and specialist Counter-Terrorist Security Advisers. Such measures aim to deter hostile interest and minimise the impact of an attack, and are likely to include restricting access, increasing the frequency of patrols, bag searching etc.

65. 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 must form an integral part of testing overall Business Continuity plans, as described in 'Security Policy No. 1: 'Governance and Security Approaches', (MR4).

MANDATORY REQUIREMENT 19

Departments and Agencies must ensure that all establishments in their estate put in place effective and well tested arrangements to respond to physical security incidents, including appropriate contingency plans and the ability to immediately implement additional security controls following a rise in the Government Response Level.

To comply with this requirement Departments and Agencies must:

- Implement the baseline CT requirements set out in supporting guidance to this Security Policy at all establishments in their estate;
- Identify an appropriate and proportionate range of incremental measures for each site that can be applied immediately in response to any increase in the Government Response Level;

- Develop appropriate Counter-Terrorist contingency arrangements and plans (as part of wider Business Continuity Planning) setting out the procedures to be followed in the event of an incident or imminent terrorist threat. Local emergency services, CPNI and specialist Counter-Terrorist Security Advisers should be consulted and plans should be aligned with any multi-agency contingency plans, where appropriate;
- Test their CT arrangements and contingency plans and take action to correct any identified issues. Establishments assessed to be at HIGH risk from terrorist attack must test their CT arrangements annually; MODERATE risk sites must test their arrangements at least every two years;
- Report the results of any tests of CT arrangements in the Annual Report to the Head of Department, and report any issues or lessons learned to the Cabinet Office in the annual Security Risk Management Overview.

Responding to Critical Incidents

66. Departments and Agencies need to be confident that they have put in place effective physical and procedural controls to mitigate and respond to any type of security incident, including terrorist attack.

67. If an establishment is identified as being at immediate threat of terrorist attack, the police and security authorities will inform the Department and may take control of the scene. This can be either pre, during or post-incident depending on circumstances and may require careful handling to avoid compromising intelligence and evidence.

MANDATORY REQUIREMENT 20

Departments and Agencies must be resilient in the face of physical security incidents, including terrorist attacks, applying identified security measures, and implementing incident management contingency arrangements and plans with immediate effect following a change to the Government Response Level.

To comply with this requirement Departments and Agencies must:

- Immediately impose a pre-determined set of additional physical security controls following any increase in the Government Response Level;

- Ensure that appropriate and resilient arrangements are in place for the management of any critical incident, including assigned roles and responsibilities and effective decision-making channels;
- Develop a strategy for communicating with staff, emergency responders and the media (also including consideration of handling enquiries from concerned family and friends). All staff must be made aware of the current Response Level and given instructions on how to respond to different types of security incident;
- Develop search plans for each establishment and plans for responding to incidents out of regular hours, as appropriate;
- Report to the Head of Department summarising steps taken and additional controls implemented following any change to the Government Response Level. Any issues or lessons learned should be reported to the Cabinet Office in the annual Security Risk Management Overview.

Annex One:
Definitions of Government Protective Markings

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 this 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

Supplementary markings (e.g. national caveats, descriptors, code words etc.) may be applied to protectively marked material to indicate additional information about its contents, sensitivity and handling requirements. Detailed information about special handling requirements is set out in supplementary material accompanying this framework.

VERSION HISTORY

SPF Version 8 – April 2012

This edition of the overarching policy framework (Tiers 1-3) remains unchanged. Several underpinning documents (tier 4) have been revised.

SPF Version 7 – October 2011

Version 7 of the policy framework was substantially revised. The following table indicates how the former 68 Mandatory Requirements (MRs) map against the 20 outcome focussed MRs set out in Version 7.

SPF Version 7 - onwards MR Structure	SPF Version 6 - Apr 2011 MR Structure
MR 1 SECURITY ORGANISATION	**3 – Board Level Responsibilities** **4 – DSO Responsibilities** **9 – DSU Training** **35 – IA Roles and Responsibilities**
MR 2 RISK MANAGEMENT APPROACHES	**5 – Risk Management Approaches** **32 - Managing Information Risk**
MR 3 CULTURE, EDUCATION AND AWARENESS	**1 – Education and Awareness for Staff** **9 – Protective Security Culture** **21 – Personal Responsibilities for Safeguarding Assets**
MR 4 MANAGING AND RECOVERING FROM INCIDENTS	**9 – Reporting of Security Incidents** **21 – Security Breach System** **49 – Disaster Recovery Planning** **70 – Business Continuity**
MR 5 ASSURANCE AND REPORTING	**6 – Self Assessment and Systems of Assurance** **7 – Annual Security Returns** **8 – Audit and Review** **34 – Statement of Internal Control** **69 – CT Assurance Statements**

MR 6 **INFORMATION SECURITY POLICY**	**31 - Information Security Policy** **10 - International Security Agreements** **11 - Government Protective Marking System (GPMS)** **12 - Legal Requirements** **15 - FOI**
MR 7 **GOVERNMENT PROTECTIVE MARKING SYSTEM**	**10 - International Security Agreements** **11 - Government Protective Marking System (GPMS)** **16 - Need to know principle** **18 - Material originating outside the HMG** **19 - Universal controls** **20- Special handling**
MR 8 **RISK ASSESSMENT AND ACCREDITATION OF ICT SYSTEMS**	**32 - Managing Information Risk** **33 - Business impact levels** **14 - HMG IA no 6 – Protecting personal data** **36 - Accreditation and audit** **37 - Compliance checks – RMADS**
MR 9 **TECHNICAL CONTROLS**	**39- Codes of connection and technical controls** **40- Cryptography** **41- Eavesdropping and Electro-Magnetic Countermeasures** **42- Remote working/mobile media** **45- Secure Disposal**
MR 10 **PROCEDURAL MEASURES**	**38 - Authentication controls** **46 - Personnel security** **48 - Education, training and awareness** **42 - Mobile working**
MR 11 **DELIVERY PARTNERS AND SUPPLIERS**	**2 – SPF Compliance among Delivery Partners and Suppliers** **31 - Information Security Policy DPs & 3PS** **43 – Procurement**
MR 12 **MANAGING AND REPORTING SECURITY INCIDENTS**	**9 – Reporting Incidents** **21 – Security Breach System** **44 - Reporting ICT Incidents**

MR 13 **RECRUITMENT CHECKS AND NATIONAL SECURITY VETTING**	**23 – BPSS compliance** **24 – National Security Vetting compliance** **26 – Clearance Decisions**
MR 14 **ONGOING PERSONNEL SECURITY MANAGEMENT**	**22 – Applying Personal Security Controls** **25 – National Security Vetting Issues** **27 – National Security Vetting Aftercare**
MR 15 **APPEALS**	**28 – National Security Vetting Appeals** **MR 29 - Notifying GSS of Legal Challenges**
MR 16 **SECURITY RISK ASSESSMENT**	**50- Defence in Depth** **51- Storage of Sensitive Assets** **55- Building Security** **62- Operational Requirements**
MR 17 **INTERNAL CONTROLS**	**47 – Physical Security of ICT Assets** **52- Secure Containers** **53- Secure Rooms** **54- Officer Areas**
MR 18 **BUILDING AND PERIMETER SECURITY**	**56- Physical Access Control** **57- Physical Access Control** **58 - Access Control Policies** **59- Incoming Mail** **60- Manned Guarding** **61- Perimeter Security**
MR 19 **PREPARING FOR CRITICAL INCIDENTS**	**64- Categorisation of the Government Estate** **65- Government Estate Response Level System**
MR 20 **RESPONDING TO CRITICAL INCIDENTS**	**67- CT Protective Security Policy and Plans** **68- Testing CT Arrangements**

The following Mandatory Requirements have been removed:

- **MR 30** (reporting security vetting records) – this data is available through other arrangements;
- **MR 63** (use of CCTV in accordance with the DPA) - refers to statutory obligations that do not need to be further mandated through security policy.

CONTACT DETAILS

The Cabinet Office Government Security Secretariat (GSS) is responsible for developing and communicating the Security Policy Framework, drawing on expert inputs from across the government security community, including the interdepartmental Centre for the Protection of National Infrastructure (CPNI) and the National Technical Authority for Information Assurance, CESG.

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

Publication date: October 2011