Security Policy Framework

Contents

Risk management in government

1. General principles and approach

1.1 All Government Departments and Agencies ***must*** adopt a risk management approach to their protective security arrangements, including, as a minimum requirement, a detailed security risk register. This document provides guidance on general approaches and principles for managing risk, and where they apply, mandatory requirements for specific security risk management methodologies.

Mandatory requirements, risk and Departmental policy

1.2 It is important to note that the Security Policy Framework, of which this guidance forms a part, sets out a series of minimum mandatory requirements (or "green boxes") for protective security and business continuity management. Whilst Government Departments and Agencies must meet these minimum requirements, it should be stressed that these are the minimum, and it is expected that organisations will need to manage their risks accordingly, and in many cases, will be expected to exceed the minimum requirement in certain areas. This is likely to correlate to the need to manage risks related to organisational specific, perhaps unique, areas of business (e.g. nuclear security or witness protection). To this extent Departments and Agencies must use the framework to develop their own tailored security policies, based not only on the minimum mandatory requirements, but also on the firm principles of risk management, proportionality and cost effectiveness. In doing so organisations will also have to address any statutory security requirements, for example Data Protection, as well more specific legislation, such as that around handling firearms, toxic materials etc.

General approaches to risk

1.3 Different approaches to risk are required to meet different purposes and Government organisations will need to employ different risk management methodologies to manage their risk effectively.

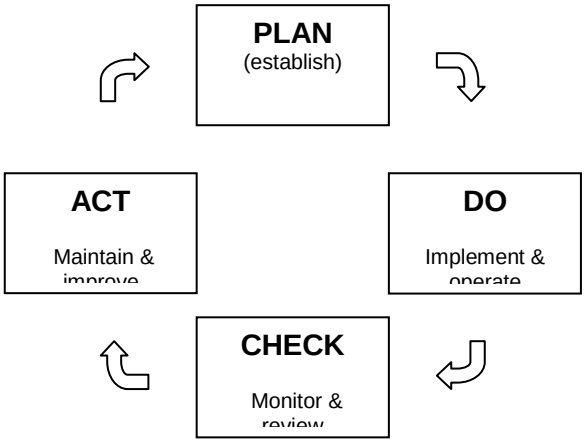
The risk management principles set out in the HM Treasury's "Orange Book" offers a general risk management approach based on the achievement of objectives and is considered good practice for Departments and Agencies.

The Orange Book should be used in conjunction with other risk management material such as the Green Book which is available on HM Treasury's website. The Green Book offers advice on the appraisal and evaluation of policies, programmes and projects to support effective policy making and resource allocation and promote the public interest. This should be used to prepare business cases for public sector expenditure.

In addition to these approaches, Departments and Agencies will need to employ specific methodologies for the management of security risks.

The risk management cycle (PDCA)

1.4 Risk management process should be managed on a general four point continuous cycle of: Plan, Do, Check and Act (PDCA model).



Using the above model HMG protective security may be summarised in the following manner:

Plan (establish protective security regime)	Establish protective security policy, including objectives, processes and procedures relevant to managing security risks in accordance with HMG mandatory minimum requirements (green boxes), taking into account the organisations overall business objectives and any statutory requirements.
Do (implement, operate, manage)	Implement, operate and manage the above policy, controls, processes and procedures.
Check (monitor and review)	Assess and measure process performance against above policy, objectives and report findings for management review ('Head of Department' annual report and annual security return to Cabinet Office on mandatory minimum requirements).
Act (maintain and improve)	Take corrective and preventative action based on results of internal audit process, peer networks, intelligence received, central guidance/policy and other relevant information, to achieve continual improvement

Calculating the level of risk

1.5 A fundamental element with this PDCA risk cycle is the need to calculate and re-assess levels of risk to organisational assets (people, information and infrastructures/systems). This is essential before correct polices, processes and measures can be adopted. Protective security risk is calculated by assessing the threat and vulnerability of identified and critical assets, and how the loss or compromise of such assets could impact on the business. The below risk matrix provides a general guide as to how overall risk can be calculated. For specific calculations relating to the different elements of protective security please refer to the section below on Personnel, Physical and Information Risk.

Level of vulnerability	**Level of Threat**					
	Very High Grade 1	High Grade 2	Significant Grade 3	Moderate Grade 4	Low Grade 5	Negligible Grade 6
Very High	Very High	High	Medium	Medium	Low	Very low
High	High	High	Medium	Medium	Low	Very low
Medium	Medium	Medium	Medium	Medium	Low	Very low
Low	Low	Low	Low	Low	Low	Very low
Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very low
	R		I	S		K

Risk management method

1.6 Risk management is a structured, common sense approach to providing cost effective, proportionate and relevant protective security to the Confidentiality, Integrity and Availability for all protectively marked and other valuable HMG assets. The theory involves thorough analysis and assessment enabling organisations to determine what specific security controls are required to achieve an appropriate level of protection for its assets. Critically, the process ***must*** include the means of monitoring application and effectiveness, and all major steps and decisions should be carefully and comprehensively documented – organisation ***must*** as a minimum have a detailed risk register (see 1.7 below) and must produce an annual report on protective security to their Head of Department/Management Board. This section identifies a number of steps required in protective security risk management, in summary these are:

1) Identify assets

2) Value assets

3) Determine the threat

4) Determine the vulnerability

5) Determine impact (from loss or compromise)

6) Review existing or establish mitigating controls

7) Consider security in the round

8) Continuous review

[Redacted]

Step 6 – Review existing/establish security controls to protect against loss to Confidentially, Integrity and Availability.

Risk is correlation between threat, vulnerability and impact of loss/compromise. Security controls should be designed to reduce risk to an acceptable level. Therefore security controls should be designed to reduce the vulnerability and thereby reduce risk to an acceptable level. The judgement of what risk is acceptable must take into account the value of the asset, including what impact it would have should it be lost/compromised (see step 5).

Suitable security controls will either need to be established in relation to the risk assessment, or existing security control will need to be reviewed. Existing security controls may be judged as being:

> **Appropriate** – There is no need to implement or change existing control, but consideration should be given to the added value of the controls when taken collectively
>
> **Excessive** – Consider reducing security controls appropriate to the level of protection required, thereby reducing the cost of the controls while being careful not to increase the risk of compromise to an unacceptable level
>
> **Inadequate** – The risk to the asset is unacceptable. Consider what security controls need to be implemented to meet the minimum requirement or reduce the risk in some other way, for example by transferring the most sensitive asset to a site with appropriate security controls.

Integrity and Availability.

Controls for Confidentiality can contribute to the protection of Integrity and Availability, however, separate considerations should be given to those areas, for example, appropriate contingency plans, such as, back up copies held off site or stand by auxiliary systems, will reduce vulnerability for loss of Integrity and Availability.

Statutory and other special handling controls

Some security controls are stipulated by law, such as firearms, munitions, nuclear and toxic materials etc, which must be followed. Also other valuable assets with clear monetary value, such as cash, computer hardware and vital ICT components, etc – in such cases a cost benefit analysis may be used when considering how much should be invested in security controls.

Step 7 – Look at Security in the round

Security controls required for each asset must not be considered in isolation. The value provided by security controls against threat and vulnerabilities should be part, often as a preliminary step, of a wider consideration of other assets. Similarly, a holistic approach must be taken with regard to physical, personal and information security controls.

Organisations should consider removing procedural security controls that do not add value to overall effect of a security regime, as long as this does not fall below the minimum requirements, or create unacceptable vulnerabilities. It is important to be clear about the added value that each measure would provide and to avoid duplication – for example, a patrolling guard force and a Intruder Detection System (IDS) may have be stipulated, however, in reality either may be sufficient to reduce the risk to an acceptable level.

Step 8 – Continuous review

Risk management is a continual process. Its components, that is asset value, threat, vulnerability, risks, protective controls and the acceptance of degrees of risk or 'risk appetite' do not remain static. Regular review is required to re-consider all these elements, particularly if there is a significant change in the threat level – either for additional, different, or a reduction in controls.

Review is particularly important following a security incident or breach. For example, after a break in when valuables have been stolen or protectively marked material compromised, in addition to repairs and corrective damage limitation, the DSO should conduct a throughout risk assessment, looking at security controls across the board, not just the immediately effected area.

Risk Register

1.7 A risk register is a simple tool enabling organisations to document and review security risks and controls. It is mandatory for Departments and Agencies to have a risk register covering their protective security arrangements, organisations may vary in the style and approach in terms of recording risks, however, registers should look to include the following: risk identifier (ID number), risk description, date, risk owner, scoring of risk (considering threat, vulnerability, as well as impact and likelihood/probability), mitigating actions,

mitigation owners, scoring of risk post mitigation (residual risk), timescales and any other additional interdependencies or relevant circumstances.

2. Personnel, Physical & Information Risk

2.1 In relation to the three elements that make up protective security (personnel, infrastructure, information/systems) there are some specific considerations in terms of risk assessment and mitigation. The Security Policy Framework identifies that the three elements of protective security must be considered together, not only in context to one another and the minimum mandatory requirements, but also in support of overall business needs, brought together in a holistic manner. Within this approach however, is must be acknowledged that each discipline has specific risk methodologies, to this extent Department and Agencies should consider, and in some cases, ***must*** adopt the following risk methodologies, for:

a) Physical security – Departments and Agencies must use either the Physical Security Baseline Controls Matrix (see MR 51) or an Operational Requirement (see MR 62) to determine levels of risk in relation to the physical and terrorist threat.
b) **[Redacted]**
c) **[Redacted]**

2.2 **[Redacted]**

Central machinery for security in government

Committee structure

1. National security, and its protective security aspects, is the responsibility of the Ministerial Committee on National Security, International Relations and Development (NSID), chaired by the Prime Minister, and its sub-committee on protective security and resilience, NSID(PSR), chaired by the Home Secretary. Details of these ministerial committees are shown at annexes A and B.

2. Other ministerial committees with interests in security are the Ministerial Committee on Domestic Affairs, sub-committee on public engagement and the delivery of services (DA(PED)), which brings together departments with security and service delivery interests and holds them to account for improved information assurance (IA) performance. The sub-committee on personal data security (DA(PDS)) specifically monitors implementation of the Data Handling Review's recommendations. Details are at annexes C and D.

3. Under these ministerial committees the Cabinet Office, through its chairmanship of the relevant official level committees and its specialist security policy staffs, exercises general oversight of security across government and, as part of the overall Cabinet Office aim to make government work better, seeks to introduce policy and process improvements and modernisation.

Cabinet Office machinery

4. The Cabinet Office is responsible for developing security policies across government and for co-ordinating their application.

- The Cabinet Secretary chairs the Official Committee on Security (SO), which is the senior official committee with overall responsibility for security in government. SO is also the National Security Authority (NSA) for dealing with international organisations such as NATO and the EU. **[Redacted]**
- The Head of Intelligence, Security and Resilience, in the Cabinet Office is also the Prime Minister's Adviser on Security, and is a member of SO.
- The Director, Security and Intelligence in the Cabinet Office, is a member of SO, and chairs its two main sub-committees **[Redacted]**
- Cabinet Office Security Policy Division provides the secretariats for SO and its two sub-committees, as well as for the Security Commission (Annex I) when it is activated and the Security Vetting Appeals Panel (Annex J). It develops protective security policies and process improvements and co-ordinates their application across government, through Departmental Security Officers. **[Redacted]**. It also provides the Government lead for security issues within the Government Security Zone of central London.
- The National Security Secretariat was set up to devise a programme for implementation of the National Security Strategy and to drive and monitor delivery across Whitehall in support of the National Security Committee (NSID).
- The Information Assurance Oversight Board, reporting to Ministers, receives reports on the performance of Government Departments in delivering the Data Handling Review measures as set out in Information Assurance Standard No. 6 – Protecting Personal Data and Managing Information Risk and National IA Strategy.
- The Information Assurance Delivery Group, chaired by the Government CIO and reporting to the IA Oversight Board, focuses on delivery of the Data Handling Review and implementation of the National IA Strategy, articulates the wider IA business needs, establishes the Common Good requirement for funding IA capabilities, and determines the need for new IA policies and standards (Annex H).
- The Central Sponsor for Information Assurance is a Cabinet Office division reporting to the Government's Chief Information Officer, responsible for setting policy for IA across Government, ensuring the co-ordination of Government needs, mandating the compliance and audit framework, and policing the outcome.

[Redacted]

ANNEX A – Ministerial Committee on National Security, International Relations and Development (NSID) Composition - **[Redacted]**

ANNEX B – Ministerial Committee on National Security, International Relations and Development Sub-committee on Protective Security and Resilience (NSID(PSR)) Composition - **[Redacted]**

ANNEX C – Ministerial Committee on Domestic Affairs Sub-committee on Public Engagement and the delivery of services (DA(PED)) - **[Redacted]**

ANNEX D – Ministerial Committee on Domestic Affairs Sub-Committee on Personal Data Security (DA(PDS)) - **[Redacted]**

ANNEX E – **[Redacted]**

ANNEX F – **[Redacted]**

ANNEX G – **[Redacted]**

ANNEX H

INFORMATION ASSURANCE DELIVERY GROUP (IADG)

Composition

The Group will be chaired by the Government CIO and will comprise principally Senior Information Risk Owners (SIROs) and senior representatives from Government. Stakeholders from industry and professional institutions will also be invited to attend as required. The membership will seek to reflect the requirements of the broad IA agenda. Attendance will be by personal invitation from the chairman and no substitutes will be permitted. Initially, membership will be:

HMG's Chief Information Officer (Chair)

Cabinet Office, Intelligence, Security & Resilience

[Redacted]

[Redacted]

Department for Transport

Department for Work and Pensions

Ministry of Defence

National Police Improvement Agency

Northern Ireland Office

Department of Health & NHS

Department for Communities and Local Government

Ministry of Justice

Home Office

HM Revenue and Customs

Terms of Reference

To drive the Government's Information Assurance (IA) agenda forward.

Objectives:

1. To ensure delivery of the actions from the report on Data Handling Procedures in Government, including changing the culture with regard to data handling.
2. To implement the broader agenda of information assurance as embodied in the National IA Strategy
3. To assess and report progress

ANNEX I

The Security Commission

The Security Commission was established in 1964 with the following terms of reference as announced on 23 January 1964 by the Prime Minister (Sir Alec Douglas-Home):

> "If so requested by the Prime Minister to investigate and report upon the circumstances in which a breach of security is known to have occurred in the public service, and upon any related failure of departmental security arrangements or neglect of duty; and, in the light of any such investigation, to advise whether any change in security arrangements is necessary or desirable."
>
> (Hansard cols 1271-3).

A statement by the Prime Minister (Mr Wilson) on 10 May 1965 widened the terms of reference to cover circumstances where there might be reason to think that a breach of security had occurred.

On 26 March 1969 the method and terms of reference were modified when the Prime Minister announced:

> "After consultation with the Rt Hon Gentleman, the Leader of the Opposition, I have revised the procedure for deciding whether or not a case involving a prosecution under the Official Secrets Act should be referred to the Security Commission. In future, when a breach of security has led to prosecution, the Chairman of the Security Commission will receive a statement outlining the facts of the case and will be asked to give his opinion on whether an investigation by the Commission would be likely to serve a useful purpose. I will then consult the Rt. Hon Gentleman taking into account the views expressed by the Chairman of the Commission before deciding whether or not to refer the case to the Commission.
>
> In any other case of known or presumed breach of security, I would decide in the light of the circumstances whether or not its significance warranted my consulting the Chairman of the Security Commission and the Rt. Hon Gentleman on the question of whether it should be referred to the Security Commission."
>
> (Hansard col. 311).

The full Commission comprises a panel of seven, from which three or four members, including the Chairman, are normally chosen when the Commission is asked to investigate a suspected breach of security.

ANNEX J

Security Vetting Appeals Panel

An independent Security Vetting Appeals Panel exists to provide a final means of challenging a decision to refuse or withdraw security clearance. It is available to hear appeals from individuals in departments and other organisations, or contractors' employees working for those departments and organisations, who have exhausted the internal appeals process and remain dissatisfied with the outcome.

Terms of Reference

1. The current policy on security vetting as announced in the Prime Minister's statement to the House of Commons on 15 December 1994, is that in the interests of national security, safeguarding Parliamentary democracy and maintaining the proper security of the Government's essential activities, no one should be employed in connection with work the nature of which is vital to the interests of the state who:

- is, or has been, involved in, or associated with any of the following activities:
  - espionage,
  - terrorism,
  - sabotage,
  - actions, intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means; or

- is, or has recently been -
  - a member of any organisation which has advocated such activities; or
  - associated with any such organisation, or any of its members in such a way as to raise reasonable doubts about his or her reliability; or

- is susceptible to pressure or improper influence, for example because of current or past conduct; or

- has shown dishonesty or lack of integrity which throws doubt upon their reliability; or

- has demonstrated behaviour, or is subject to circumstances which may otherwise indicate unreliability.

2. Where an employee of a department, agency or other organisation specified in the Annex is aggrieved by the withdrawal or refusal of security clearance, and has exhausted appropriate internal appeal mechanisms, they may appeal to the Security Vetting Appeals Panel. The Panel will:

i. examine whether the appeal falls within the remit of the Panel; if so, it will:

ii. examine the procedure by which the vetting authority obtained and assessed the information underpinning the adverse vetting decision;

iii. examine the merits of the vetting decision, taking into account the interests of national security and the rights of the individual;

iv. produce a report of their recommendations for the Head of Department or equivalent; and

v. produce a report for the complainant. As far as is possible, this should duplicate that sent to the Head of Department or equivalent.

For further details on the Security Vetting Appeals Panel refer to the Personnel Security section on the SPF.

Working with Ministers

Risks

1. Ministers and their Private Offices have access to a great deal of sensitive information and often work in busy and pressurised environments. This inevitably increases vulnerabilities in terms of protecting information appropriately. Risks which Private Offices may face include:

- The requirement for a Minister to work on sensitive material whilst travelling / in their constituency / during official trips.
- A greater requirement to share sensitive information with both departmental / non-departmental staff.
- Private Offices may have a higher volume of visitors than other offices and security will be a greater risk where offices are open plan.
- Ministers (and the subject areas they deal with) attract a lot of media attention. Any security breaches will cause significant reputational damage and may harm National Security.

2. This note should be used as a 'quick-reference' guide for use by Ministers and their staff, but detailed advice on asset protection and information security can be found within the Security Policy Framework.

Protecting documents and other protectively marked assets

Where is it possible to work on documents?

3. Protectively marked assets should not be worked on anywhere where the contents might be overlooked or otherwise noticed, and they should not be left unattended in any public place, such as, a restaurant, hotel, taxi or on public transport. They should not be entrusted to the custody of a member of the public, for example, by being left in a hotel safe, or left locked in an unattended vehicle.

4. It is not good practice to work on official documents while travelling on public transport. Opening any container containing official information will introduce a degree of vulnerability, as would communicating about such subjects by telephone or insecure email.

5. However, a pragmatic approach should be adopted. **[Redacted]**

6. **[Redacted]**

Taking papers to meetings / home working

7. Ministers and civil servants are discouraged from taking documents **[Redacted]** out of the building, unless using the documents for a meeting as it increases the risk of compromise. They must be returned to the building to be stored appropriately as soon as possible.

8. **[Redacted]**

9. **[Redacted]**

10. **[Redacted]**

11. **[Redacted]**

12. **[Redacted]**

13. **[Redacted]**

[Redacted]

14. **[Redacted]**

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**

    d. **[Redacted]**

15. **[Redacted]**

16. **[Redacted]**

[Redacted]

17. **[Redacted]**

18. **[Redacted]**

19. **[Redacted]**

20. **[Redacted]**

[Redacted]

21. **[Redacted]**

[Redacted]

22. **[Redacted]**

a) **[Redacted]**

[Redacted]

b) **[Redacted]**

c) **[Redacted]**

d) **[Redacted]**

e) **[Redacted]**.

f) **[Redacted]**

[Redacted]

g) **[Redacted]**

[Redacted]

[Redacted]

23. **[Redacted]**

[Redacted]

24. The GCS is operated by the Government Car and Despatch Agency, an Executive Agency of the Department for Transport. **[Redacted]**

Personnel Security

25. It is a long standing principle that Government Ministers, MPs, Peers and members of the judiciary are not subject to security vetting.

26. When sharing protectively marked information above CONFIDENTIAL with departmental staff, you should check that recipients have appropriate security clearances to see the information. For further details please see Security Policy No. 3: Personnel Security.

27. **[Redacted]**

Advice and guidance

28. The Permanent Secretary has overall responsibility for security within the department. Departmental policy may vary from central guidance and if you have any concerns or queries you should approach the Departmental Security Officer in the first instance, who will refer matters to the Permanent Secretary if appropriate.

Roles and Responsibilities

Staff Responsibilities

1. All staff are responsible for protective security in one way or another. This can range from wearing security passes and exercising appropriate vigilance against suspicious items or behaviour, to applying the controls described throughout the Security Policy Framework, and the specific responsibilities placed upon individuals by the Civil Service Management Code, Data Protection Act and other relevant legislation such as the Official Secrets Act.

2. All staff should be familiar with these responsibilities and obligations and Departments and Agencies should ensure that on recruitment they receive suitable security induction and training. They should be reminded of these responsibilities at suitable intervals throughout their careers.

3. Line managers have an important role to play in ensuring that staff are aware of their responsibilities and that these are being met. Similarly, Heads of Management Units will want to be satisfied that the appropriate security controls are being adhered to across their parts of the organisation and may well be asked to contribute to any compliance or incident reporting regime established by the Departmental Security Officer (DSO).

Lead Officials for Security

4. The Security Policy Framework requires that Departments and Agencies will have the following nominated officials with specific responsibilities for security:

- **A board level lead** for protective security generally.
- A designated **Departmental Security Officer (DSO)** who exercises day to day responsibility for all aspects of protective security (physical, personnel and information).

- A designated **Information Technology Security Officer (ITSO)** responsible for the security of information in an electronic form.
- A designated **Communications Security Officer (ComSO)** if cryptographic material is handled.
- **[Redacted]**

5. And, in respect of managing information risk and personal data:

- An **Accounting Officer** with overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.
- A designated **Senior Information Risk Owner (SIRO)** responsible for owning departmental information risks.
- **Information Asset Owners**: suitably senior named individuals responsible for each identified information asset (e.g. database or ICT system).
- **Accreditors**: responsible for impartial assessment of the risks of departmental information systems and for formally accrediting such systems.
- **Chief Information Officer**: A senior manager, preferable at Board-level who advised the Board how best to exploit technology to deliver the organisation's strategic objectives, and provides strong strategic leadership for the organisation's IT community and its investment in the technology.
- **Chief Technology Officer**: The professional technology lead, reporting to the Chief Information Officer and responsible for IT strategy, IT architecture, IT policies and standards, technology assurance and IT professionalism.

6. This section describes the roles and responsibilities of those lead officials with responsibility for protective security.

Security – a devolved responsibility

7. Security is a devolved responsibility – each Head of Department or Agency and Minister are responsible for the security of their organisation and its assets, by recourse to the centrally driven protective security policy described in the Security Policy Framework. Protective security is a complex issue and one that will inevitably touch every part of a

department or other official body; it requires appropriate organisation and structures to be put in place.

8. Given the diversity of Departments and Agencies no one security organisation or structure will be suitable for all. However the Security Policy Framework specifies some minimum roles and responsibilities (listed above). The Head of Department or Agency and Departmental Security Officer (DSO) should exercise overall responsibility for protective security generally. A number of other roles are required to exercise responsibility for specific information security and data handling responsibilities.

9. Departments and Agencies will want to allocate and determine these roles in a pragmatic way that delivers the most appropriate and effective security regime across the entirety of their organisation. In particular, Departments and Agencies will want to ensure that there is sufficient strategic oversight of risk management and protective security issues to ensure that a holistic security regime is in place that balances information, personnel and physical security considerations.

Clearances

10. All officials with lead responsibilities for security should be appropriately security cleared and inducted to reflect the level of access to protectively marked and/or other sensitive assets that they will have.

Security Roles

Board Level Leads

11. As described the Head of Department or Agency is ultimately responsible for the security of their organisation. Consequently they may choose to act as the Board level lead for security or invite a suitably senior colleague to support them in this area.

Key Tasks

12. The purpose of the Board Level Lead is to act as the champion for all security issues and factor security into the organisations business planning. **[Redacted]**

a) **[Redacted]**
b) **[Redacted]**
c) **[Redacted]**
d) **[Redacted]**
e) **[Redacted]**
f) **[Redacted]**
g) **[Redacted]**
h) **[Redacted]**
i) **[Redacted]**

13. **[Redacted]**

a) **[Redacted]**
b) **[Redacted]**
c) **[Redacted]**
d) **[Redacted]**
e) **[Redacted]**

Departmental Security Officer (DSO)

14. Departments and Agencies must have a Departmental Security Officer (DSO) with overall responsibility for day to day protective security issues. The DSO will ensure that appropriate levels of security are in place in the Department or Agency in order to protect assets and contribute to overall national security.

15. The DSO will act as the lead official responsible for co-ordinating the department's response to security related matters. This will include: assessing and making judgments in relation to risk; drafting and delivering security policies and procedures; and monitoring compliance and providing assurance.

[Redacted]

16. **[Redacted]**

a) **[Redacted]**
b) **[Redacted]**
c) **[Redacted]**
d) **[Redacted]**
e) **[Redacted]**
f) **[Redacted]**
g) **[Redacted]**
h) **[Redacted]**
i) **[Redacted]**
j) **[Redacted]**
k) **[Redacted]**
l) **[Redacted]**

[Redacted]

17. **[Redacted]**

Information Technology Security Officer (ITSO)

General Responsibilities

18. The ITSO is responsible for developing and implementing IT Security policy and procedures within their Department or Agency in accordance with HMG policy standards and guidance as laid out in the Security Policy Framework **[Redacted]** the business needs of the organisation. This must be undertaken in conjunction with the DSO, SIRO and those responsible for IT services (including Managed Service Providers).

19. The ITSO will also be responsible for the organisation of IT security, liaison with HMG security and IT authorities on local and National Security policy issues, providing advice on security reviews and investigations relating to IT issues, as well as being responsible for IT security awareness education and training.

20. The DSO/ITSO may choose to perform the role of the Accreditor themselves or to appoint an individual to carry out the specific function of accreditation on their behalf. See paragraph 30 for further details. The ITSO, the ComSO, the DSO, SIRO and Accreditor(s) will need to interact to ensure overall security is maintained.

[Redacted]

21. **[Redacted]**

a) **[Redacted]**
b) **[Redacted]**
c) **[Redacted]**
d) **[Redacted]**
e) **[Redacted]**
f) **[Redacted]**
g) **[Redacted]**
h) **[Redacted]**
i) **[Redacted]**
j) **[Redacted]**
k) **[Redacted]**

Training and expertise

22. The level of IT and IT security training required to fill an ITSO post will depend on the job requirements and competencies of that post. In addition to the IT training (probably based on the IT Infrastructure Library or similar) the ITSO would receive for the technical aspects of their career, specialist IT Security and general security training as required. The Department or Agency should provide training on their IT systems and general security training.

23. The National School of Government (NSG) runs courses on IT security in line with government policy, which are suitable for ITSOs, both at Introductory and Practitioner level. An ITSO would be expected to meet the requirements set out by the Institute of Information Security Professionals (IISP) for Associate Membership (A.Inst.ISP), together with IISP annotation indicating competence in the HMG environment (equivalent to the ITPC Certificate of Infosec Competency).

[Redacted]

General Responsibilities

24. If a Department handles cryptographic material, it must have a designated ComSO. The ComSO is responsible for developing and implementing Communications and Cryptographic policy and procedures within their Department or Agency in accordance with HMG policy and Standards **[Redacted]**. This must be undertaken in conjunction with the DSO, SIRO **[Redacted]**.

25. The ComSO will also be responsible for the organisation of Communications and **[Redacted]**, liaison with HMG security authorities and communication authorities on local and National Security policy issues, advising security reviews and investigations on communication **[Redacted]**, as well as being responsible for communication **[Redacted]**.

26. The ComSO will work closely with the ITSO, the DSO, SIRO and accreditors to ensure overall security is maintained.

[Redacted]

27. **[Redacted]**

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

28. **[Redacted]**

[Redacted]

29. **[Redacted]**

- **[Redacted]**
- **[Redacted]**

[Redacted]

30. **[Redacted]**

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

31. **[Redacted]**

Information Risks and Information Assurance

32. Information risks and information assurance must be managed effectively and to do so Departments and Agencies are required to nominate a number of lead officials to exercise specific responsibilities.

[Redacted]

33. **[Redacted]**

[Redacted]

34. **[Redacted]**

[Redacted]

35. **[Redacted]**

[Redacted]

36. **[Redacted]**

Training and expertise

37. The Government runs courses to meet the needs of accreditors, both at Introductory and Practitioner level, at the National School of Government. An Accreditor would be

expected to meet the requirements set out by the Institute of Information Security Professionals (IISP) for Associate Membership (A.Inst.ISP), together with IISP annotation indicating competence in the HMG environment (equivalent to the ITPC Certificate of Infosec Competency).

Independent DSO Status Letter

CabinetOffice

[Redacted]

To: [name]
[Address] Date: xxxx

Dear [name]

DEPARTMENTAL SECURITY OFFICER POST

1. Thank you for your letter of [date] requesting that the Cabinet Office consider whether it is appropriate for [organisation's name] to have a DSO in its own right.

2. Our function here is to ensure that protective security policy across the Government sector is co-ordinated and developed in line with emerging threats to Government assets, their vulnerabilities and on the basis of managing risk. Generally this policy is set out in the Security Policy Framework (SPF), issued under the authority of the Official Committee on Security (SO). Departments are required to implement central policy and advice as appropriate. As to whether a department should retain a single DSO, or where it has a number of agencies of other subsidiary bodies delegate the function, we would expect departments to consider a number of factors. At the risk of making some obvious points, perhaps I could set these out.

3. It is important that departments have clear governance arrangements across their delivery chains which are able to provide assurances that security requirements are being met. These arrangements must reflect their accountability and their overall responsibilities, including those for protecting their own assets – people, property and information – and those assets of others for which they have a responsibility, such as shared information. It is for the department to assess the risks to its business and people and to put in place measures that are necessary and proportionate to mitigate the risks and provide necessary protection. Where a department has

agencies enjoying a measure of independence the extent to which it can delegate responsibilities for security will depend on the terms of the agency's framework document or letters of delegation. We recognise that there may be benefits in moving responsibilities closer to operational units, in terms of more detailed understanding of the risks to the business. However, in general, unless a department can delegate all its responsibilities in this area, we would expect the departmental DSO to retain a role in relation to its agencies. There are clear benefits in departments coordinating advice and guidance to their agencies and other delivery partners where shared services or opportunities for economies of scale are involved.

4. **[Redacted]**

I look forward to your response.

Yours sincerely,

[Redacted]

ANNEX A - [Redacted]

Security breach management

1. Introduction

What is a security breach?

1.1 A security breach may be defined in general terms as the compromise of Confidentiality, Integrity and Availability of HMG assets. However, security breaches may include a range of situations which could lead to damage, such as operational effectiveness, harm to reputation - both organisationally and personally - and in the most extreme cases can lead to prejudice of national security, result in a crime and even endanger lives. All breaches, or potential breaches, of security ***must*** be taken seriously and investigated in a swift and proportionate manner. HM Government takes all breaches of security very seriously.

1.2 The unofficial 'leaking' of information to the press, lobbyists, special interest groups or anyone is a breach of confidentiality and in contravention of the Civil Service code – for specific guidance please refer to **[Redacted]** and the **<Civil Service Code>.** 'Losses' are also considered a breach, and are normally associated with the compromise of integrity or availability, resulting from theft, fraud, lack of care or poor security.

Roles and responsibilities

1.3 All staff (including contractors) have a personal responsibility to ensure that they do not commit security breaches themselves, they ***must*** also report any concerns that security policy is not being adhered to, and breaches are either being committed or there is a high likelihood they are being committed. Moreover, if there are strong grounds to believe that security breaches may occur, for example, due to vulnerable procedures or individuals, this should also be reported.

1.4 The Departmental Security Officer (DSO) ***must*** ensure that there is an adequate system for detecting, reporting and responding to security breaches. The following guidance provides good practice on breach management and also identifies areas that must be followed.

1.5 Senior managers have a responsibility to ensure that all security breaches are taken seriously and sufficiently investigated, and where necessary, corrective, disciplinary and

or legal proceedings are actively pursued.

2. Breach policy

2.1 Departments ***must*** ensure that all staff are made aware that any breach of security policy, whether accidental or deliberate, will lead to disciplinary/administrative action, and in extreme or persistent cases, termination of employment/services and if appropriate, criminal proceedings.

2.2 Departmental breach policy ***must*** be aligned to and be consistent with personnel/ Human Resources policy and employment law.

2.3 Breach policy ***must*** be highlighted and freely available to all departmental staff, either via internal intranet sites or other departmental communication tools. It is best practice to include a briefing of breach policy as part of any general and or security induction programme, as well as at any re-fresher training.

3. Breach management system

What is a breach system?

3.1 A breach system is a way of managing the appropriate controls and actions to report and respond to a security breach. **[Redacted].**

3.2 Breach systems are often based around sensitivity of the asset compromised; the Protective Marking System can provide a useful guide when considering appropriate sanctions **[Redacted]** However, it is important to note that there can be a range of factors to consider and each case ***must*** be considered on its own merits.

3.3 Many Departments use a points based system to log and report the type and number of breaches committed – this is useful for determining proportionate sanctions, looking at trends within the Department, as well as providing a record of repeat offenders, who may face additional penalties for persistent infringement. Departments ***must*** be able to

supply the overall numbers of security breaches, both physical and electronic, in response to Parliamentary Questions. Whilst there is no requirement to provide any further details beyond the numbers, in response to PQs, it is considered good management practice to keep a detailed record.

4. Reporting breaches

Local reporting

4.1 The DSO ***must*** ensure that formal reporting arrangements exist so that all security breaches are brought to their attention immediately. A quick reaction can help to contain or minimise the consequences of a leak, loss or breach, and can greatly assist in any subsequent investigation and possible recovery of assets.

Central reporting

4.2 All leaks ***must*** be reported to the Directorate of Security and Intelligence (DSI) Secretariat at Cabinet Office following the guidance found in **[Redacted].**

4.3 **[Redacted]**

4.4 Any significant losses of data, particularly large amounts of personal data, ***must*** be reported to Cabinet Office immediately. If an incident does involves large amounts of personal data it may also need to be reported to the Information Commissioner's Office and to the Ministry of Justice - **[Redacted]**

Other reporting

4.5 It may be necessary to notify other bodies/individuals/third parties in regard to a specific breach in order to help reduce onward impact – this is particularly important for data losses involving personal information. **[Redacted]**

4.6 If the owner of the compromised asset is a foreign government or international organisation, the ***Foreign and Commonwealth Office must be consulted immediately*** regarding informing the country or organisation involved.

4.7 **[Redacted]**

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

5. Reacting to a security breach

5.1 When reacting to a breach, the response should be quick, but at all times proportionate to the assessed damage or consequences. It is important for the DSO to establish whether the breach is a 'loss' or a 'leak' as procedures and reporting differ slightly **[Redacted].** For losses the DSO should ensure that all losses are brought to the attention of those responsible for departmental finance. Guidance on accounting for losses is contained in **<HMT Government Accounting Guidance>.**

5.2 If the breach involves more that one department, for example the compromised asset belongs to another department, or it belongs to an interdepartmental committee, it is important to establish who is best placed to act as lead department. In very serious cases the Cabinet Office should be consulted and if necessary they will either act as lead department, or decide who should lead.

[Redacted]

5.3 **[Redacted]**

6. 'Whistleblowing'

6.1 Departments ***must*** have a clear, stated and available 'whistleblowing' policy. Staff ***must*** have recourse to consult with a welfare or similar independent arbiter/ officer. In most cases individuals should raise concerns initially with line managers, if it is inappropriate or cannot be resolved by managers then referrals should be made to the appropriate (e.g. HR/Personnel/Corporate Services) senior staff up to and including Permanent Secretary level. If individuals are not satisfied, after seeking referral though the management chain, there is recourse to the independent Civil Service Commissioners.

6.2 The Public Interest Disclosures Act, sometimes known as the 'Whistleblowers Act', provides employees, both in the private and public sectors, with protection against victimisation should they 'blow the whistle' in certain circumstances. It allows individuals to make disclosures about crime, breach of legal obligation, miscarriage of justice, danger to health and safety or the environment, and the cover up of any of these issues. For more information please refer to **[Redacted]**.

Appendix A – [Redacted]

Training and Awareness

1. The Security Policy Framework requires that Departments and Agencies ensure that:

a) Board members responsible for security undergo security and risk management familiarisation upon appointment – see Training Opportunities for Board Level Security Leads.

b) All DSOs are given a **[Redacted]** security briefing from Cabinet Office **[Redacted]** on appointment, and have either attended the relevant training courses before, or at the earliest opportunity after, appointment. – see paragraphs 8-10.

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

d) Security education and awareness must be built into all staff inductions, with regular familiarisation thereafter – see Delivering a training and education programme for all staff.

e) There are plans in place to foster a culture of proportionate protective security - see Delivering a training and education programme for all staff.

f) There is a clearly stated and available policy, and, to allow for independent and anonymous reporting of security incidents – see **Security Breach Management**.

Background

2. Basic security training and awareness is needed by all employees, including those without direct access to protectively marked information, so that all are familiar with the basic principles of protective security and alert to threats to national security and other sensitive assets (for example citizen data). Those with specific security responsibilities, with access to protectively marked assets and management at all levels will require regular training and briefing specific to the controls associated with the handling of protectively marked material. It is also important to ensure that certain categories of employees in junior grades, who may handle large quantities of protectively marked assets, or undertake sensitive duties (for example, messengers, couriers, guards and clerks), receive adequate security education and supervision.

3. Generally, detailed knowledge of national security rules and procedures and training in their implementation can be confined to those with access to protectively marked assets. And, since good protective security is at its most effective when implemented 'top-down', line and personnel managers will need an overall knowledge that is likely to require less emphasis on detail, but with a particular emphasis on management's responsibilities for the security and safety of employees and other resources or assets.

4. Specific protective security training is required for those individuals or groups:

a. Who are ultimately responsible for security and risk management at Board level within their organisations.

b. Who are Departmental Security Officers (DSOs) and Information Technology Security Officers (ITSOs) or their deputies.

c. Who are otherwise employed as security specialists, and will therefore require a thorough and extensive security training programme

d. Who require security training courses and briefings tailored to their particular role, for example, those responsible for the protection of employees and property against the threat from terrorism and sabotage. The recommended route for government information assurance specialists is to follow the government-approved training (currently laid down by the Infosec Training Paths and Competencies (ITPC) scheme). From April 2009, The Institute of Information Security Professionals (IISP) is taking over responsibility for ITPC certification, and will annotate membership as ITPC-compliant for those who achieve membership of the IISP as either Associate Member or Full Member, and meet the requirements laid down by Government.

Security Culture and Awareness

5. All HMG Employees have a collective responsibility to ensure that government assets (information, property and staff) are protected in a proportionate manner from terrorist attack, and other illegal or malicious activity.

6. The SPF Mandatory Requirement 1 states that all staff must understand relevant requirements and responsibilities placed upon them by the SPF and that they are properly equipped to meet them. MR 9 requires security education and awareness to be built in to all

staff inductions, with regular updates thereafter and that the departments should foster a culture of proportionate protective security.

7. Departments and Agencies should determine the best way to meet these requirements depending on their organisational culture and particular business needs. **[Redacted]**

8. **[Redacted]**

Training Opportunities for Board Level Security Leads, DSOs and DSU Staff

9. Cabinet Office Security Policy Division (COSPD) is working with the National School for Government, **[Redacted]** and others to develop a training pathway for Board Level Security Leads, DSOs and their deputies. This will build upon the existing training provision available **[Redacted]**, the NSG, BSI and others summarised at Annex A**.**

10. **[Redacted]**

Training for Board Members responsible for security and risk management

11. Board level security leads' responsibilities will include:

- Securing Board buy-in for security, changing and influencing the culture of their organisation in relation to security, and seeking assurance that plans are in place.
- Ensuring compliance, particularly with regard to the requirements of the SPF.
- Managing risks

12. Board members will want to ensure that they are sufficiently informed to discharge these responsibilities (and others as described in the Roles and Responsibilities guidance which supports MR 3 within the SPF), and that they have a sound, strategic understanding of the risks their organisations face, including the current security issues via briefings from Cabinet Office, DSOs, **[Redacted]** and pan-government networks (such as the SIRO network).

Training for Departmental Security Officers and Deputies

13. Critical elements of the DSO role include:

- Knowing the needs of the business and where security fits in.
- Putting in place and monitoring compliance with the SPF mandatory requirements, incremental security controls and relevant legislation.
- Having a sound understanding of risk management, the threat and critical parts of their organisation.
- Knowing where to get help and information: the Cabinet Office, **[Redacted]**, police, etc.
- Knowing how to respond to critical incidents.

14. DSOs, their deputies and Departmental Security Units (DSU) staff generally will need to ensure they are sufficiently informed to carry out these roles (and others described in the Roles and Responsibilities Section (see MR 3) via relevant professional training. On appointment they should advise Cabinet Office Security Policy Division **[Redacted]** that they have taken on the role and arrange for a joint induction briefing.

15. DSOs, deputies and DSU staff must consider their training needs and identify relevant training opportunities (see Annex A).

Delivering a training and education programme for all staff

16. Over and above the training of staff with specific security responsibilities DSOs will want to establish a security awareness and training programme for all members of staff generally. Overall the objective should be to establish and develop an organisational culture that is alive to security and promotes security as an important business enabler.

17. This will include the handling of protectively marked assets, other official assets and specific requirements associated with the handling of citizen data. Requirements relating to the 2008 Data Handling Review are described in detail at Annex B.

18. Timing the delivery of training and education is an important element in implementing and maintaining an effective awareness programme. The following arrangements represent an ideal which departments and agencies should achieve so far as is possible. DSOs will, in reality, often need to delegate responsibilities to branch and unit security officers and line

management, and may need to call on the services of the organisation's personnel and training branches, sections or units.

19. The needs of a new employee to a department or agency should be assessed and met as soon as possible after recruitment. This should include basic security education and other training as determined by the duties of the post. General security principles and minimum mandatory requirements are available to all staff via the public version of the Security Policy Framework (on the Cabinet Office website) which can be referenced at staff induction.

Ongoing training and refreshers

20. Departments and Agencies should have in place a continuing programme of security education for all employees. This should serve both to remind them of the threats to security and to bring them up-to-date with developments including, where appropriate, lessons drawn for recent espionage cases, security breaches and terrorist incidents. The programme should ensure that all employees receive some security education at regular and defined intervals. Employees with specific security responsibilities should also be able to attend security training courses at appropriate intervals so that their knowledge of, and competence in, using rules and procedures is kept up-to-date.

On posting and promotion

21. Where applicable, security education and training should be an intrinsic part of the preparation for a new post. Employees moving for the first time to posts with responsibilities for and tasks involving protectively marked assets, should be fully briefed on the security implications of their work, and the correct practices to be adopted, prior to taking up their posts. Employees already experienced in handling protectively marked assets should receive specific training when they are given significant additional tasks or responsibilities. In particular, further training will be required on management training courses. This type of training should include a clear security education and training element, clarifying the respective responsibilities of line and personnel managers for the security of employees in their charge. Other examples of situations that will require additional security education and training include:

a. Postings as security specialists
b. Postings abroad

c. Postings involving more sensitive work
d. Postings involving different procedures
e. Postings on shift work
f. Posting to out-stations remote from headquarters
g. Promotions involving increased management and/or security duties
h. Postings involving contact with the media and representational duties
i. The introduction of new or replacement technology.

On the implementation of new procedures

22. It is especially important that any changes in security rules and procedures, that are likely to have been introduced because a weakness has been detected or because new equipment is being used, should be made known to all employees involved.

Suggested content of a security education and training programme

23. When considering the content of an awareness programme, the DSO may wish to include the following:

[Redacted]

a. **[Redacted]**

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

- **[Redacted]**
- **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

[Redacted]

g. **[Redacted]**

h. **[Redacted]**

- **[Redacted]**
- **[Redacted]**

i. **[Redacted]**

j. **[Redacted]**

k. **[Redacted]**

Methods of delivery

24. There are a number of different methods that can be used for the implementation of a security education and training programme.

Talks, briefings, seminars and courses

25. The choice of method will depend on the specific training requirement, which must first be clearly defined, on the nature of the target audience and on the degree to which it is desirable that the individuals in the audience should participate. But whatever the chosen method, there should always be an opportunity for some form of audience participation, if only provision for questions.

a. As a general guide, if only one subject is to be covered, a talk may be the most appropriate method of delivery. It is useful to confirm the audience's understanding of the talk with subsequent discussion. It is also important to consider the size and composition of the audience. For example, it may be difficult to pitch a talk to capture and retain the interest of groups comprising widely different grades or specialisms. Large audiences may pose problems: audibility, reduced impact of the message on the individual, and the tendency for individuals to feel anonymous in a crowd and therefore to listen and contribute less.

b. A seminar or informal talk may be useful when a greater degree of audience participation and discussion is possible and desirable, for example:

- When persuading senior management of the importance of promoting good security practice
- When introducing employees to the security requirements of a specific task

c. If a wider variety of topics of general interest needs to be covered, a presentation with different speakers may best hold the attention of an audience, and help them to distinguish between the different subjects

d. When a greater amount of information is to be conveyed, and the individuals need to understand and apply it, a course may be desirable, with opportunities for practical exercises to ensure that the audience understands and retains the information

Audio visual and other presentation aids

26.

a. With both presentations and courses, frequent question and answer periods provide a change of pace and the opportunity of digesting the information. Such periods need to be guided or stimulated by those running the events. Appropriate visual aids, for example, overhead projector, electronic presentation and slides should be used to reinforce the message. Clear and simple aids should be used which whilst enhancing the presentation, do not distract the audience.

b. Films and videos provide a particularly effective way of informing large and/or dispersed audiences of the various threats to security and of making them aware of their security responsibilities. They can be used as visual aids during a course or presentation or be the main focus of a separate security session. A film or video should never be used in isolation, but must be set firmly in its security context by the presenter, otherwise the audience will be inclined to judge the film solely on its entertainment value and obtain little or no security benefit. The showing of a film should always follow a brief introduction that describes its purpose and points to look out for. A discussion of the value of the film and the security lessons it highlights

should follow. Where appropriate guidance notes for the use of presenters are not provided with the film, departments and agencies should compile their own.

c. A number of security education films and videos are available, many of them sponsored by the **[Redacted]** MOD. They should be chosen with the audience in mind, for example, civilians may not relate to a film featuring uniformed characters, and should be suited to the audience's expertise and seniority.

Adding security education sessions to other training courses

27. Departments and agencies should be alert to the possibility of adding security education sessions, films or videos to other types of training courses, for example, induction or management training.

Providing forms of security education material other than training courses

28. There are a number of other methods by which security education material can be circulated to employees outside of formal and informal presentations, seminars and training courses.

a. Posters bearing security messages are not intended to teach lessons, but to remind individuals of the threats to security and of the principal security controls necessary to counter them. Their impact tends to be temporary so posters should not only be prominently displayed but also frequently changed.

b. Stickers are intended to remind employees of their personal responsibility for the maintenance of security when using specific items of security equipment, for example, the secure use of the telephone or fax. They should be placed on, or adjacent to, the equipment concerned. They should not be placed on items of security furniture.

c. Desk calendars and other devices bearing security messages are also intended to remind individuals of their personal responsibilities for security, particularly for those procedures most closely related to desk work; for example, locking away protectively marked assets, ensuring that assets have correct protective markings.

d. Circulars and Newsletters may be used for:

a. promulgating security rules and amendments
b. relating instance of breaches of security and the lessons to be learned from them see **Security Breach Management** for details.
c. encouraging the avoidance of breaches, perhaps by periodic circulation of breach information within a department or agency, that might serve as a way of promoting a sense of competition between branches, sections and divisions to achieve the highest security standards
d. warning individuals of specific or topical threats to security and providing guidance to counter them
e. providing a channel of communication with individuals on security matters

Annex A

	TRAINING PROVIDER	COURSE TITLE
Governance, Compliance and Risk Management[1]	**National School of Government (NSG)**	Management of Risk (Accredited)[2] Advanced Diploma: Risk Assurance and Internal Audit Management Diploma Level: Corporate Governance and Risk Management (IIA Module 5) Understanding and Managing the Risk of Fraud
	[Redacted]	**[Redacted]** **[Redacted]**
	British Standards Institute (BSI)	Internal Auditor BS2259 (Business Continuity) Internal Auditor ISO 27001 (Information Assurance) Lead Auditor ISO 27001 (Information Assurance)
Personnel Security	**NSG**	Baseline Personnel Security Standard[3] 1 day Physical and Personnel Security course (new course planned for 2009-10)
	[Redacted] **[Redacted]**	**[Redacted]** **[Redacted]**
	BSI	BS7858 Security Screening Training
Information Assurance	**NSG**	Annual Sunningdale Accreditors' Conference Risk Management and Accreditation Document Set[4] Diploma Level: Business Information Systems Auditing (IIA Module 4) NSG moving to modular delivery in 2009-10 – a move that should lend itself better to DSO provision.

[1] The NSG provide a wide variety of course on audit and risk management; many of these are components of project and corporate management courses.
[2] Course also includes component on Business Continuity
[3] Designed for HR practitioners
[4] Includes modules on Risk Management

	BSI	Introduction to ISO 27001 Practitioner Certificate in Information Risk Management (PCiiRM) Understanding the Requirements of ISO/IEC 27002 (17799) and the ISO/IEC 27000 series ISEB Certificate in Software Asset Management Essentials Best Practice in Information Security Risk Management using BS7799-3 ISEB Certificate in Information Security Management Principles (CiISMP) Implementing ISO 27001 Lead Implementer ISO 27001
[Redacted]	**[Redacted]** **[Redacted]**	**[Redacted]** **[Redacted]** **[Redacted]**
Physical Security	**[Redacted]** **NSG**	**[Redacted]** 1 day Physical and Personnel Security course (new course planned for 2009-10)
[Redacted]	**[Redacted]**	**[Redacted]**
Business Continuity	**BSI**	The Business Continuity Foundation Course Developing and Managing Business Continuity Exercises Writing the Business Continuity Plan Understanding PAS 77 Business Continuity Basics Implementing BS25999 – A practical guide Crisis and Incident Management Business Impact Assessment BS25999 Executive Workshop

Annex B

Data Handling Review Requirements – Security Training

In June 2008 the Cabinet Office published the final report of the review into Data Handling Procedures in Government. This set out a requirement for all staff with access to protected personal data should successfully complete basic information risk awareness training, on appointment and annually thereafter. Cabinet Office have produced an e-learning package, Protecting Information, which may be used as part of this programme and is designed to be relevant to all staff, not just those with access to protected personal data. However, departments and agencies should set this awareness in context for their own environment.

The Data Handling Review and subsequent work has also defined requirements for other roles, including the Senior Information Risk Owner (SIRO) and Information Asset Owner (IAO).

For more information on the e-learning package or other training being developed, please contact CSIA on csia@cabinet-office.x.gsi.gov.uk.

International Protective Security Policy

Introduction

1. UK Protectively Marked information should only be disclosed to foreign governments, international organisations and commercial or industrial entities based overseas, in cases where:

a) There is a clear need to know;

b) The overseas partner has demonstrated both the ability and willingness to protect UK protectively marked material; and,

c) Appropriate protective security arrangements have been agreed with the recipient nation / organisation.

Reciprocal arrangements apply to classified material provided to the UK by overseas entities.[5]

2. The following sections set out the policy framework for the exchange of protectively marked assets overseas, including the role of the centre and departmental responsibilities.

[5] The term 'protectively marked' is used throughout this paper to refer to UK information / assets bearing a security classification; foreign information bearing a security classification **[Redacted]** is termed 'classified' information / assets.

1. UK National Security Authority

3. All NATO and EU Member States are required to establish a National Security Authority (NSA) to act as the focal point for matters related to security policy and the protection of material bearing a security classification. The Official Committee on Security (SO) is the UK NSA for international security policy issues. **[Redacted]** Cross-government policy coordination is undertaken by Cabinet Office Security Policy Division (COSPD). Other departments and agencies may represent the UK in specialist international fora acting as the Designated or Competent Security Authority (DSA/CSA).

4. The UK NSA was established to represent the UK in NATO security bodies. Its remit now includes EU and other multi-lateral security fora, and negotiation of bilateral Security Agreements for use across government (undertaken by COSPD). The NSA objectives are:

a) To ensure that UK protectively marked information exchanged internationally receives appropriate protection;

b) To ensure that international organisations / fora handling or generating classified information implement appropriate security regimes consistent with UK standards;

c) To ensure that any classified information provided by international organisations or other countries and held or processed by the UK government, agencies or industry is protected appropriately.

5. To achieve a) and b), the UK NSA negotiates security standards and procedures both bilaterally and through international security fora (such as NATO and EU security committees). These arrangements provide a pan-government framework for the exchange of UK protectively marked information with foreign governments, based on the assurance that information will be protected in accordance with common minimum security standards. In the case of defence information, the MoD has negotiated a number of similar security Arrangements. Objective c) is achieved by cascading information about these standards to departments, agencies and industry, through this Framework and specific security notices; audit and assurance procedures are set out in SPF Security Policy No.1: Governance, Risk Management and Compliance.

6. ***Departments and Agencies remain individually responsible for the security of the information they hold.*** Any decision to disclose UK protectively marked information to

overseas partners must be taken on a risk managed basis, balancing the need to know against an assessment of whether the nation concerned is both willing and able to protect UK protectively marked information.

7. Departments and agencies ***must*** ensure that adequate security arrangements have been agreed before any UK protectively marked information is released. **[Redacted]** Where no established links exist and depending on the level of classification concerned, appropriate protective security arrangements could take the form of a bilateral Security Agreement / Arrangement or a subject-specific Memorandum of Understanding (MOU) or equivalent exchange of letters. Departments and Agencies should consult the UK NSA / COSPD before negotiating any new security arrangement with a foreign nation concerning the protection of assets at **CONFIDENTIAL or above**.

Appropriate security arrangements **must** *be in place before any disclosure of UK protectively marked assets to overseas governments, international organisations, or industry.*

Any protectively marked assets **must** *be appropriately marked and sent only to those States that demonstrate the ability and willingness to protect such assets from compromise.*

COSPD **should** *be consulted before negotiating any new security arrangement with a foreign nation concerning assets at* ***CONFIDENTIAL or above****.*

2. International Agreements

8. The UK is party to various international agreements covering the handling of classified material originated by international organisations and foreign governments, along with reciprocal arrangements for UK protectively marked assets sent overseas. These agreements commit the parties to apply equivalent, mutually agreed security standards for the protection of information bearing a security classification and to provide assistance for personnel and industrial security checks.

9. The UK has security obligations in connection with:

a) Bilateral Security Agreements or Arrangements

b) International Defence Organisations (principally NATO)

c) Atomic Information Agreements

d) European Union institutions and agencies

e) Other international organisations

10. Every effort has been made to ensure consistency between the standards set out in this Framework for UK protectively marked information and security requirements for the protection of foreign classified information. However, there are differences.

11. The purpose of each agreement, its security regime and the lead UK department are set out below. Any differences between these security regulations and the provisions in this Framework for UK assets are set out in the sections concerning Personnel Security and Information Security.

For guidance on the carriage of protectively marked UK assets overseas refer to Section 5 of the SPF guidance concerning the Government Protective Marking System and Asset Control.

2.1 Bilateral Security Agreements / Arrangements

12. The UK Government has signed a number of bilateral Agreements (treaties) and Arrangements (Memoranda of Understanding, MOUs) for the mutual protection of

information bearing a security classification. These Agreements / Arrangements may be general (i.e. government-wide in scope) or, more commonly, limited to a specific subject / sector (e.g. defence protectively marked information). Whilst MOUs entail moral and political commitments, treaties also impose legal obligations. Though enforcement mechanisms are different in each case, in practice these obligations should be considered to be equally binding on the participants.

13. **[Redacted]**

14. Security Agreements / Arrangements commonly fall into two categories: General Security Agreements / Arrangements (GSAs), which are negotiated by COSPD and set out common minimum standards for the mutual protection of all information bearing a security classification exchanged between the Governments or any commercial or industrial organisations in the two countries; and Security Agreements / Arrangements (SAs) negotiated by the MoD which are limited to the protection of protectively marked defence information exchanged between the participants. Both address the following subjects:

a) equivalent markings and protective security standards;
b) restrictions on how and when information at different levels of classification can be used, transmitted and disclosed;
c) rules and notification procedures governing access to classified material by staff, contractors or visitors;
d) reciprocal industrial security arrangements and requirements for placing contracts;
e) protocols following the loss or compromise of classified material; and,
f) dispute resolution procedures.

15. The existence of a security agreement / arrangement in no way implies an obligation to share protectively marked information overseas; rather it provides an agreed mechanism to facilitate any exchanges.

16. The MoD has negotiated over 25 SAs with overseas partners **[Redacted]** Advice on the existence and provisions of these Arrangements may be obtained from MoD-Def Sy-S&T Ind 1.

17. COSPD has agreed GSAs **[Redacted]** and further negotiations are ongoing both bilaterally and multi-laterally within fora such as the EU. Further information and advice about GSA terms and the progress of negotiations can be obtained from COSPD.

18. Classified assets originated by foreign governments should be afforded the same level of protection determined by its equivalent UK protective marking **[Redacted]**

2.2 International Defence Organisations

19. The UK is a member of several international defence organisations (IDOs), although in practice its principal commitment is to the North Atlantic Treaty Organisation (NATO). The Central Treaty Organisation (CEATO) and South East Asian Treaty Organisation (SEATO) are now both defunct. The dormant Western European Union (WEU) continues to function as a European defence and security organisation, though most WEU functions have been subsumed into the European Security and Defence Policy (ESDP) pillar of the European Union.

20. IDO Member States ***must*** adhere to the organisation's security regulations when handling information or assets relating to that organisation. The principle IDO security regulation is ***North Atlantic Treaty Organisation (NATO) C-M(2002)49.*** This regulation is closely aligned to the security provisions in this Framework. Any differences or inconsistencies are explained in the sections below concerning Personnel Security and Information Security. Further detailed guidance about handling NATO classified information can be obtained from The Control Officer, International Documents Registry, MoD.

21. International Defence Organisations use similar protective markings to those used by the UK, prefixed to identify the originating organisation, for example, NATO SECRET

2.3 [Redacted]

22. **[Redacted]**

23. **[Redacted]**

24. **[Redacted]**

25. **[Redacted]**

26. **[Redacted]**

2.4 European Union Institutions and Agencies

27. Various European Union institutions, agencies and decentralised bodies require access to classified information to perform their duties. **[Redacted]**

28. Most EU agencies fall under the remit of either the EU Council or the EU Commission. Both bodies have security responsibilities and have developed their own security regulations[6]. These regulations are similar to the NATO Security Regulations and, like NATO, they entail security obligations on the Member States (see the sections on Personnel Security and Information Security).

Departments and Agencies that exchange protectively marked information with an EU body, or that receive and process EU Classified Information (EUCI), ***must*** *notify the COSPD to ensure that an appropriate security agreement is in place and that they are applying the correct security regulations.*

Departments and Agencies should consult the UK NSA / COSPD for guidance on regulations governing the handling of classified information originating from other EU Member States.

2.5 Other International Organisations

29. Various other international organisations produce classified information requiring protection under treaties or other arrangements. **[Redacted]**

30. The Organisation for Joint Armament Co-Operation (OCCAR) was established in 1996 and given legal status through the OCCAR Convention in January 2001. Member States are Belgium, France, Germany, Italy, Spain and the UK. The OCCAR mission is to facilitate and manage collaborative European armament programmes on behalf of the Member States and other States who choose to participate in a particular programme activity. **[Redacted]**

31. Further guidance about handling foreign classified information, can be obtained from the appropriate security regulations of the organisation concerned or from the UK NSA / COSPD.

[6] Respectively: Council Decision 2001/264/EC; and Commission Decision 2001/844/EC

3. Personnel Security (International)

This Section should be read in conjunction with SPF <Security Policy No. 3: Personnel Security>.

32. Various International Agreements allow for the exchange of protectively marked information with foreign governments or international organisations (see section 2, International Agreements). Under these Agreements, the UK is obliged to apply mutually agreed personnel security controls before allowing individuals access to, or knowledge or custody of, classified information originated by foreign governments or international organisations. The UK is also obliged to undertake security vetting checks for UK nationals directly recruited by, or seconded to, certain international organisations (e.g. NATO).

33. Personnel security clearance procedures for access to classified information originated by a foreign government or international organisation are broadly equivalent to standard UK practices. **[Redacted]**

34. The following sections highlight the differences between UK practices for access to protectively marked information, and those required under international commitments. Departmental responsibilities and key contact points are identified. Further information can be obtained from the UK NSA / COSPD.

3.1 Bilateral Security Agreements

35. Under the terms of bilateral Security Agreements / Arrangements, the parties mutually agree to recognise Personnel and Facility Security Clearances (PSCs / FSCs) issued by the other country. Individuals may be granted access to classified information from the other country provided they have a 'need-to-know', hold the requisite level of security clearance and have been briefed on the protective security controls.

36. An SC clearance is required for UK nationals to access foreign originated information at the equivalent level to UK CONFIDENTIAL or above **[Redacted].** A DV clearance is

required for UK nationals to have any access to foreign originated information at the equivalent level to UK TOP SECRET.

37. Dual nationals of which one element is UK can have full access to UK protectively marked information **[Redacted]** provided that:

a) They have a 'need to know';

b) They hold the appropriate level of security clearance;

c) Any potential conflicts of interest identified during the security vetting process are managed appropriately.

38. **[Redacted]**

39. Where UK resident non-UK Nationals or individuals of dual nationality (neither of which is British) need access to any protectively marked assets bearing a National Caveat which excludes their own nationality / dual nationality, the information originator must be consulted before access is given. COSPD should be consulted if there is any doubt about allowing a dual national access to either UK protectively marked assets bearing a national caveat, or to foreign classified information.

40. NATO and EU Member States, or nations with which the UK has signed a Security Agreement / Arrangement, may request assistance in carrying out security clearance checks of their nationals who have been resident in the UK **[Redacted]**

41. **[Redacted]**

3.2 NATO and EU Personnel Security Requirements

[Redacted]

42. **[Redacted]**

[Redacted]

Security Clearance Requirements:

43. Where UK nationals (or in some cases foreign nationals resident in the UK) are recruited by NATO, the EU (Council, Commission) or their respective Agencies and executive bodies, the UK Government may be invited to provide appropriate security clearance certificates **[Redacted]**

44. **[Redacted]**

45. **[Redacted]**

46. **[Redacted]**

47. **[Redacted]**

48. **[Redacted]**

[Redacted]

49. **[Redacted]**

50. **[Redacted]**

[Redacted]

51. **[Redacted]**

52. **[Redacted]**

53. **[Redacted]**

[Redacted]

54. **[Redacted]**

[Redacted]

55. **[Redacted]**

56. **[Redacted]**

57. **[Redacted]**

58. **[Redacted]**

59. **[Redacted]**

[Redacted]

60. **[Redacted]**

61. **[Redacted]**

62. **[Redacted]**

63. **[Redacted]**

[Redacted]

64. **[Redacted]**

65. **[Redacted]**

66. **[Redacted]**

Withdrawal or withholding of security clearance

67. **[Redacted]**

68. Individuals who have a security clearance refused or withdrawn may be eligible to appeal against the decision - refer to the section concerning the Security Vetting Appeals Panel (SVAP) process in the SPF Security Policy No. 3: Personnel Security.

3.3 [Redacted]

3.3.1 [Redacted]

[Redacted]

69. **[Redacted]**

70. **[Redacted]**

71. **[Redacted]**

[Redacted]

72. **[Redacted]**

[Redacted]

[Redacted]

[Redacted]

[Redacted]

73. **[Redacted]**

[Redacted]

74. **[Redacted]**

75. **[Redacted]**

[Redacted]

[Redacted]

76. **[Redacted]**

77. **[Redacted]**

[Redacted]

78. **[Redacted]**

[Redacted]

79. **[Redacted]**

80. **[Redacted]**

[Redacted]

81. **[Redacted]**

82. **[Redacted]**

3.3.4 European Atomic Energy Commission

83. The UK acceded to the Treaty establishing EURATOM on 1 January 1973. It is bound by EURATOM Regulation Number 3 which implements Article 24 of the Treaty and provides for the protection of EURATOM classified information (ECI).

84. SC clearance is required for all UK nationals recruited by or seconded to EURATOM requiring access to EURATOM CONFIDENTIAL or SECRET information.

85. OCNS retains responsibility for the vetting of all UK nationals directly recruited by EURATOM (many having been previously employed in the UK civil nuclear industry), other than those recruited from other UK Government departments and agencies. FCO should therefore forward to OCNS any applications received from the Commission for clearance action in respect of EURATOM (DG TREN) Safeguards officials. In the latter case, the parent department or agency should undertake appropriate vetting for individuals seconded

to EURATOM and issue an EU security clearance certificate using the template in **[Redacted]**.

4. Information security

This Section should be read in conjunction with the SPF paper concerning the Government Protective Marking System and Asset Control.

86. Under the agreements listed in Section 2 and **[Redacted]**, the UK is obliged to safeguard classified information received from foreign governments and international organisations to mutually agreed standards. Reciprocal provisions cover the handling of UK protectively marked information provided to foreign governments and international organisations. Standard clauses include the protective marking of assets, approved methods of transmission and storage, registration of highly classified material and asset handling procedures in general. Whilst most requirements are broadly equivalent to UK best practice as set out in this Framework, there are differences. Key contact points for each agreement / arrangement are listed in Section 3 and should be consulted in any case of doubt as to the appropriate practices.

Mandatory requirements for access to UK Protectively Marked Information

87. Non-UK nationals working for foreign governments, contractors and international organisations may be given access to UK protectively marked assets provided that:

a) Their parent nation / organisation has demonstrated the ability and willingness to protect UK assets;

b) The individual has a proven need to know;

c) The individual holds the appropriate level of security clearance; and

d) The information has been confirmed as appropriate for release to nationals of the country concerned.

88. Non-British locally engaged staff at UK Diplomatic Missions or Service contingents overseas may be permitted access to UK protectively marked assets provided that they have been granted an appropriate security clearance, have been briefed about the protective

security controls required (including any local sensitivities), and that the material is releasable to their parent nation in accordance with any national caveat.

89. Departments and agencies are responsible for the security of the information they hold. Any decision to release UK protectively marked information overseas should be taken on a risk management basis. No information should be disclosed until the Department or Agency is satisfied that adequate security arrangements are in place for the protection of UK protectively marked information. Departments and Agencies should consult the UK NSA / COSPD before negotiating any new security arrangement with a foreign nation concerning the protection of assets at CONFIDENTIAL or above.

[Redacted]

90. **[Redacted]**

UK protectively marked assets sent to overseas governments, contractors or international organisations ***must*** be prefixed "UK". Descriptors ***must not*** be added to protectively marked information sent overseas.

91. Classified information supplied by another nation should be safeguarded to a similar standard as that afforded to UK protectively marked assets of an equivalent level **[Redacted]** any information exchanged under the terms of a Security Agreement / Arrangement must not be disclosed or transmitted to any third party Government, individual, contractor, or to any international organisation, without the prior written consent of the originating party. Public information requests under the UK Freedom of Information Act (2000) that concern classified information originating overseas are dealt with in section 4.6.1.

Overseas Disclosure of Assets Marked PROTECT

92. The marking 'PROTECT' is a sub-National Security marking used to designate information that requires a basic level of protection, but where it would be disproportionate to

apply the security measures necessary for RESTRICTED material in the UK. PROTECT is not recognised by bilateral or multilateral Security Agreements / Arrangements, or by international organisations, and there are no foreign equivalent markings. Unless project-specific security arrangements have been agreed concerning the handling of PROTECT, foreign partners will have no understanding of how such information should be protected and safeguarded from disclosure. **[Redacted]** Where appropriate, the information should be accompanied by a copy of the RESTRICTED handling conditions set out in Appendix 6 to the SPF List X Contractual Process (Appendix 6: Guidance for Overseas Contractors on the Protection of UK Restricted Assets) to ensure that foreign partners apply appropriate security controls.

[Redacted]

Personal data

93. The security of personal data held or processed by off-shore partners was considered by the 2008 Data Handling Review[7]. The Review set mandatory minimum standards for the protection of personal data including marking it as PROTECT when it is processed or stored within Government or its delivery partners, including overseas partners. The aggregation or accumulation of personal data may merit additional protective security controls as any loss or compromise is likely to have a bigger impact and cause greater damage than the loss of one piece of unclassified data. Therefore an adjustment to the impact level, but not necessarily the protective marking, may be required. **[Redacted]**

94. Departments and Agencies intending to off-shore personal data are required to undertake a risk assessment and submit their plans for scrutiny by the Information Assurance Delivery Group (IADG) and, ultimately, for approval by the DA(PDS) Ministerial Committee. Departments and Agencies should also consider contacting the Information Commissioner's Office (ICO) for advice.

95. Personal data supplied by another nation should be safeguarded to a similar standard as would be afforded to equivalent UK information in accordance with the Data Protection Act (1998). This may require the recipient to add a protective marking to

[7] Data Handling Procedures in Government: Final Report - June 2008 - http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf

unclassified foreign material in accordance with the guidance set out in Security Policy No. 2 – Protective Marking and Asset Control.

96. See section 5.1 for rules concerning the placement and management of protectively marked contracts overseas.

Carriage and Transmission of UK Protectively Marked Information Overseas

97. The following sections set out specific guidance on the marking of UK assets sent overseas **[Redacted]** For guidance on the carriage and transmission of protectively marked UK assets overseas - refer to Section 5 of the SPF guidance concerning the Government Protective Marking System and Asset Control.

98. **[Redacted]**

4.1 Special Handling Instructions

99. The need-to-know principle is fundamental to all aspects of security. Where it is necessary to reinforce this principle special handling instructions (caveats) may be applied to further limit access to designated groups. **[Redacted]**

[Redacted]

100. **[Redacted]**

101. **[Redacted]**

102. **[Redacted]**

[Redacted]

103. **[Redacted]**

104. **[Redacted]**

105. **[Redacted]**

106. **[Redacted]**

[Redacted]

107. **[Redacted]**

108. **[Redacted]**

109. **[Redacted]**

110. It is the responsibility of the originator to decide if assets need to be disclosed to foreign governments or international organisations and, if so, the countries involved. The application of any National Caveat is designed to limit the disclosure of such assets to specific allies. Some departments and agencies may need to apply other national caveats to meet specific needs. In such cases, the originator must ensure that appropriate access and handling arrangements are in place to take account of local sensitivities and the level of protection needed to protect the assets against compromise.

111. **[Redacted]**

112. **[Redacted]**

[Redacted]

113. **[Redacted]**

114. **[Redacted]**

[Redacted]

115. **[Redacted]**

116. **[Redacted]**

117. **[Redacted]**

118. **[Redacted]**

119. **[Redacted]**

120. **[Redacted]**

[Redacted]

121. **[Redacted]**

[Redacted]

122. **[Redacted]**

123. **[Redacted]**

124. **[Redacted]**

[Redacted]

125. **[Redacted]**

[Redacted]

126. **[Redacted]**

4.3 Exchanges with NATO and the EU

NATO

127. **[Redacted]**

128. NATO regulations concerning asset handling and control are broadly equivalent to standard UK practices **[Redacted]**

European Union

129. EU Council and Commission Security Regulations address similar subjects to those set out in the NATO security policy. **[Redacted]**

130. **[Redacted]**

131. The Council Security Regulations (Council Decision 2001/264/EC) and the Commission Security Regulations (Commission Decision 2001/844/EC) are both available online.[8] The UK NSA / COSPD should be consulted in the event of any doubt as to the appropriate procedures.

132. **[Redacted]**

133. **[Redacted]**

[Redacted]

134. **[Redacted]**

135. **[Redacted]**

[8] Council: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0066:EN:PDF

Commission: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_317/l_31720011203en00010055.pdf

[Redacted]

136. **[Redacted]**

137. **[Redacted]**

138. **[Redacted]**

4.5 International Visits

Government officials

139. When an individual is required to visit countries in the context of the various Agreements / Arrangements set out in Section 2, the parent Department or Agency is responsible for the visitor control arrangements. Detailed information concerning official visits can be obtained from the respective departmental security units. The following instructions and regulations outline the procedures to be followed.

[Redacted]

140. **[Redacted]**

[Redacted]

141. **[Redacted]**

[Redacted]

142. **[Redacted]**

[Redacted]

143. **[Redacted]**

[Redacted]

144. **[Redacted]**

Other agreements

145. Formal arrangements for the issue of security clearance certificates are not always incorporated in the other agreements discussed above. Prior to the visit of a UK official, the host government or international organisation's security organisation must be informed of the individual's security clearance status and the nature of the classified information which they wish to discuss. The responsibility for providing the relevant information rests with the employing Department or Agency.

Visit by non-officials

146. An International Visit Control Office (IVCO) exists in the MoD DE&S (DDSY/PSYA IVCO). Its role is to provide advice to UK staff from List X defence contractors who have a requirement to visit establishments or contractors overseas on defence business, and need guidance on the security requirements of foreign Governments and International Organisations.

147. MoD DE&S DDSY/PSYA IVCO deal with visits by MoD officials or List X contractor staff who are required to undertake visits to NATO HQ or its Agencies. IVCO also process visit requests by List X contractor staff who are required to undertake visits to overseas government or contractor establishments involving the discussion of protectively marked information relating to defence programmes or contracts. IVCO also coordinate inward visits on defence business by foreign personnel to MoD HQ establishments and List X defence contractors. The approval for visits to List X companies involving non-defence contracts or activities is the responsibility of the relevant UK Department or Agency, liaising as required with the List X company to be visited. List X companies engaged, or likely to be engaged, on such business are advised about the security requirements for such inward visits and IVCO will have given the contractor detailed instructions on how to make use of its services.

148. Under Security Agreements / Arrangements there is a responsibility on Departments and Agencies to provide specific details to the overseas government about visits that involve access or discussion of classified information, or if the visit is to a restricted site. **[Redacted]**

149. Departments and Agencies requiring information or advice on their own responsibilities for processing visit requests may find the information contained on the MoD

DE&S DDSY/PSYA IVCO website useful.[9]

150. Alternatively they should consult the British diplomatic mission in the country to be visited. **[Redacted]**

4.6 Official Disclosure

4.6.1 UK Freedom of Information Requests

151. *Foreign classified information held by UK Departments and Agencies may be subject to disclosure under the Freedom of Information Act 2000 (refer to the Legal Guidance in SPF Security Policy No.2: Protective Marking and Asset Control). The most germane exemptions under the Act (Section 27 International Relations and Section 24 National Security) are subject to public interest balancing tests that cannot be prejudged. The possibility therefore exists that the Information Commissioner, Information Tribunal or the Courts may compel the disclosure of foreign classified information, even without the express consent of the nation concerned.* **[Redacted]**

152. **[Redacted]**

4.6.2 Release of Foreign Records to the National Archives

153. Under the ***Public Records Acts 1958*** and ***1967***, certain types of records of historical or archival significance, are selected for preservation and released to the National Archives (TNA) 30 years after the latest document was originated. Details of the arrangements for the release of International Defence Organisations (IDO) documents, and those originated by other International Organisations and foreign governments, are issued to Departmental Record Officers by the TNA as they become available.**[Redacted]**

4.6.3 Disclosure of UK Assets Sent Overseas

154. Over seventy countries around the world have implemented some form of freedom of

[9] http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/ISS/InternationalVisitsControlOffice.htm

information legislation. Most have incorporated exemptions to prevent the disclosure of information which would be harmful to international relations, or are able to protect such information from disclosure through other legislative / constitutional provisions. **[Redacted]**

[Redacted]

155. Departments and Agencies ***must*** notify COSPD about any requests from foreign governments to disclose UK protectively marked material under local freedom of information (or other) legislation.

[Redacted]

156. **[Redacted]**

[Redacted]

157. **[Redacted]**

158. **[Redacted]**

159. **[Redacted]**

160. **[Redacted]**

161. **[Redacted]**

[Redacted]

162. **[Redacted]**

[Redacted]

163. **[Redacted]**

[Redacted]

164. **[Redacted]**

165. **[Redacted]**

[Redacted]

166. **[Redacted]**

167. **[Redacted]**

168. **[Redacted]**

5. Industrial Security Overseas

This Section should be read in conjunction with SPF guidance concerning the List X Contractual Process.

169. **[Redacted]** Before a contract involving UK protectively marked information can be placed with an overseas entity, the Department or Agency concerned (the contracting authority) must be confident that:

a) the host nation of the contractor has demonstrated they are both willing and able to protect UK information;

b) the information is appropriate for release to nationals of that country; and,

c) the overseas entity has adequate security measures in place for the protection of any protectively marked information.

170. Departments, Agencies and contractors ***must*** only place contracts/sub-contracts involving information protectively marked CONFIDENTIAL or above with foreign organisations when:

a) the UK has signed a bilateral Security Agreement with the host government; or,

b) binding, project-specific security arrangements have been agreed with the host government; and,

c) the host government security authorities have confirmed that the organisation concerned has been granted a Facility Security Clearance to at least the maximum level of protectively marked information associated with the contract.

These bilateral Agreements / Arrangements stipulate that the host government's security authorities will take responsibility for the security oversight and assurance for the protection of the information that is necessary for contracted entities to meet a level equivalent to UK protective security standards.

171. Different levels of security assurance are required depending on the classification of

the material and the subject matter concerned. The process of awarding and monitoring protectively marked contracts is set out in detail in the SPF sections concerning Industrial security – Departmental Responsibilities and the List X Contractual Process. In any cases of doubt, departments and agencies should contact COSPD for guidance. MoD agencies should consult MoD DE&S DDSy/PSYA-ISS.

5.1 Placing RESTRICTED Contracts Overseas

172. Departments, Agencies and contractors may place contracts/sub-contracts up to UK RESTRICTED with overseas entities provided that the conditions in paragraph 170 have been satisfied. It is for the Contracting Authority to exercise the necessary level of diligence to ascertain whether the proposed contractor is a bona fide company with which they may confidently do business.

173. **[Redacted]**

174. The Contracting Authority should ensure that such contracts (up to RESTRICTED) include clauses providing for the security of protectively marked information passed to or generated by the contractor. It is good practice to include provisions concerning the following:

a) the contractor's responsibility for ensuring an adequate level of protection for protectively marked information or material;

b) the right of the Contracting Authority to visit and inspect the contractor's premises;

c) the rules governing whether or not parts of the contract may be sub-contracted; and if sub-contracting is permitted, how the Contracting Authority's permission is to be obtained beforehand;

d) any employees working on protectively marked aspects of the contract should have undergone basic recruitment checks including:
   - proof of identity;
   - confirming that they satisfy all legal requirements for employment;
   - verification of employment history; and,
   - criminal record checks (where possible under local laws).

e) any other security requirement the Contracting Authority may consider it

necessary to include.

175. The contract should also provide for a range of legitimate remedial actions to be taken by the Contracting Authority to promptly enforce the security requirements such as:

a) suspension of the contract, overall, or in parts;
b) removal of persons from the contract;
c) retrieval of any protectively material/information;
d) instructions to take certain actions to secure protectively marked material/information.

Maintenance of an adequate security system should be a fundamental "term" of any such contract, permitting termination for default.

176. On award of contract, the Contracting Authority ***must*** give the contractor written guidance detailing the minimum requirements for the safekeeping of the assets involved - refer to Appendix 6 to the SPF List X Contractual Process - Guidance for Overseas Contractors on the Protection of UK Restricted Assets. The contractor should also be notified of the PROTECT / RESTRICTED aspects of the material in the form of a Security Aspects Letter (Appendix 4 to the SPF List X Contractual Process - Security Aspects Letter). Unless required under the national rules of the overseas host government, Personnel or Facility Security Clearances are not required for contracts up to UK RESTRICTED level.

177. Guidance on the placement of non-protectively-marked contracts overseas is available from the Office of Government Commerce (OGC).

5.2 Placing Contracts Overseas at CONFIDENTIAL and Above

178. Contracts involving UK protectively marked assets at Confidential or above should only be awarded to contractors based overseas providing they have been granted an appropriate Facility Security Clearance (FSC). Under the terms of Security Agreements / Arrangements the host government's National Security Authority (NSA) / Designated Security Authority (DSA) is responsible for undertaking these checks and for providing security assurances to the contracting government. In the absence of a relevant bilateral Agreement / Arrangement, Departments and Agencies may negotiate alternative project

specific arrangements with the host government's security authorities.

179. Departments and Agencies ***must*** consult COSPD before negotiating any new security arrangements with a foreign nation concerning assets marked CONFIDENTIAL or above.

180. Before any assets can be released, the Contracting Authority must be assured that:

a) the contractor is suitable to access and hold such assets;

b) the appropriate contractor's employees have been suitably cleared and authorised;

c) appropriate security controls are in place within the contractor's premises for the protection of the assets involved;

d) an appropriate security agreement (general or project specific) has been signed with the host government.

181. These conditions are applicable for as long as protectively marked assets need to be held on the contractor's premises. In addition to the contractual clauses outlined in paragraphs 175-6, the contracts should make reference to the relevant Security Agreement / Arrangement and it is good practice to include standard conditions clearly stating that the contractor is responsible for implementing and maintaining appropriate protective security controls in accordance with its own national security laws and regulations.

182. Classified information received from foreign governments or international organisations can only be disclosed to overseas governments or contractors with the express written consent of the originator.

Before entering into preliminary discussions or placing subcontracts for work involving classified assets supplied by foreign governments and International Organisations, COSPD or MoD DE&S-ISS (for MoD Agencies) must be consulted.

5.3 Verification of Foreign Industrial Security Clearances

183. Under Security Agreements / Arrangements, the respective NSAs / DSAs commit to

mutually recognise Personnel and Facility Security Clearances (PSC/FSC) for commercial or industrial entities on the territory of the other party. Departments and Agencies wishing to place a contract involving UK protectively marked information (CONFIDENTIAL or above) must request the host NSA/DSA to advise whether prospective contractors have the appropriate Facility Security Clearances for the level of the contract. In the event that a contractor does not yet hold the necessary clearances, the host NSA / DSA can be requested to undertake this work, though the lead times can be significant.

184. Departments, Agencies and List X contractors seeking to verify the security clearance status of a commercial or industrial entity under the terms of a Security Agreement / Arrangement should contact UK NSA / COSPD for advice (MoD DE&S-ISS for defence contracts), providing the following information:

a) Full facility name;
b) Full facility address;
c) Mailing address (if different from b);
d) Zip code/city/country; and
e) Name of the security officer

5.4 Facility Security Clearance Requests from Foreign Governments and International Organisations

185. Commercial and industrial entities in the UK are often required to provide evidence that they hold a valid UK FSC in order to tender for, and take up, classified contracts let by foreign states and International Organisations. In such instances, the relevant sponsoring Department or Agency should only undertake FSC work in response to a request from the foreign government or International Organisation that is letting the contract. These requests will often be passed through the UK NSA to the most appropriate UK sponsor Department or Agency depending on the subject matter (identified as the Competent Security Authority, CSA). For defence contracts MoD DE&S-ISS are approached directly. For legal and practical reasons, Departments / Agencies should not initiate FSC work in response to direct requests from industry (speculative vetting).

UK Government Agencies

186. UK Government Agencies participating in international research programmes (e.g.

the EU 7th Framework Programme) should not be required to provide evidence of an FSC. Rather, the responsible Departmental Security Unit should provide an assurance (via the UK NSA) that the Agency concerned is a government body, that the employees working on the project are UK government civil servants holding appropriate Personnel Security Clearances, and that that the organisation meets the security standards necessary to hold and process information up to the relevant classification level. Departments and Agencies are reminded that NATO and EU security regulations (and the terms of bilateral Security Agreements / Arrangements) stipulate an SC clearance to access CONFIDENTIAL information.

Annex A: **[Redacted]**

Annex B: **[Redacted]**

Annex C: **[Redacted]**

Annex D: **[Redacted]**

Annex E: Contact details

ACO	**Atomic Control Office, Ministry of Defence** 1.L.06, Main Building, Horseguards Avenue, London SW1A 2HB **[Redacted]**
COSPD	**Cabinet Office Security Policy Division** Room 2.42, 26 Whitehall, London SW1A 2WH Tel: 0207 276 5649 E-mail: COSPD@cabinet-office.x.gsi.gov.uk
[Redacted]	**[Redacted]**
FCO	**Foreign and Commonwealth Office** Personnel Security Team - Security and Estates Directorate, Old Admiralty Building, London SW1A 2PA **[Redacted]**
MoD DE&S DDSY/PSYA IVCO	**Ministry of Defence Defence Equipment & Support** DE&S DDSy&PSyA - IVCO Poplar-1, #2004, Abbey Wood, Bristol, BS34 8JH **[Redacted]**
MoD-Def Sy-S&T Ind 1	**Ministry of Defence Def Sy S&T/Ind 1** Zone B, 6 Floor, Main Building, Whitehall, London, SW1A 2HB **[Redacted]**
MoD IDR	**International Documents Registry, MoD** The Control Officer, International Documents Registry, Room 041, Old War Office Building, Whitehall, London, SW1A 2EU. *Until April-October 2010, then:* The Control Officer, International Documents Registry, CTLB

	SSBC-Security **[Redacted]**, Mail Point G.M.10, Main Building, Whitehall, London, SW1A 2HB.
MoJ FOI Clearing House	**Ministry of Justice Central Clearing House** Information Directorate, Information Policy Division, 102 Petty France, London, SW1H 9AJ Tel: 0203 334 3891 E-Mail: clearinghouse@justice.gsi.gov.uk
OCNS	**Office of Civil Nuclear Security** Harwell Science and Innovation Campus Didcot, Oxfordshire, OX11 0QA Tel: 01235 432925 E-mail: OCNS.Enquiries@hse.gsi.gov.uk
UK NSA	**United Kingdom National Security Authority** (Address as per COSPD)

Annex F: Version History

TITLE OF CHAPTER / SECTION	PARA REFERENCE	SUMMARY OF CHANGES
[Redacted]	**[Redacted]**	**[Redacted]**
International Protective Security Policy	Para 94	Line added recommending departments and agencies should consider consulting the Information Commissioner's Office.
[Redacted]	**[Redacted]**	**[Redacted]**

The Government Protective Marking System and asset control

1. The Protective Marking System

1.1 The UK Government's Protective Marking System (hereafter referred to as GPMS) comprises five levels (PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET) designed to help individuals determine, and indicate to others, the necessary controls required to prevent the compromise of sensitive government assets; primarily, but not exclusively, National Security assets.

1.2 The GPMS is a cornerstone on which many other government protective security controls and considerations are based. For example, personnel security and IT security will use the GPMS as an important element in determining the necessary levels of vetting and technical controls required. The GPMS provides a good reference and start point for protective security as a whole; it is therefore critical that all staff have an awareness of the system, and for those who do handle protectively marked material, have a full appreciation of the system and how it specifically relates to their role. The universal baseline standards for all protectively marked material and the definitions for each marking can be found at Annex A and Annex B respectively.

Legal Framework

The GPMS is not a statutory scheme. Its operation therefore takes place within the framework of domestic law and its operation must comply with it. A protective marking should offer an accurate indication of the sensitivity of an asset, which includes assessing the damage, or potential damage, caused by its compromise.

1.4 **Official Secrets Act 1989 (OSA):** Damage assessment is a critical element of the OSA, most of the offences in which require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or

special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons notified under section 1 of the OSA; Crown servants; government contractors; and any person.

1.5 **Data Protection Act 1998 (DPA)**: The handling of personal data which is protectively marked must comply with the DPA. The DPA, however, contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA such as the right of access to personal data. For example, section 28 provides an exemption from the data protection principles and a number of other provisions of the DPA if it is required for the purpose of national security. But note that, although the exemption is widely drawn, it is only available to the extent that it is **required** for the purpose of national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with the DPA. Other exemptions, such as section 29 (crime and taxation) are more narrowly drawn. Whilst the presence or absence of a protective marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one applies. Departments and agencies should also have regard to the DPA, including any relevant exemptions, when sharing protectively marked personal data with other departments and agencies or pursuant to international agreements.

1.6 **Freedom of Information Act 2000 (FOIA):** Protective markings can also assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply - the definitions at Annex B provide guidance on which exemptions are likely to apply. However, it must be noted that each FOI request must be considered on its own merits and the protective marking in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle protectively marked assets, understand fully the impact of such legislation and how it relates to their role.

1.7 Organisations must ensure that staff are provided with guidance on OSA, DPA and FOIA, and that such guidance is available for them to consult thereafter, either via internal intranet or by other internal communication systems.

Further guidance

1.8 For further guidance and advice on OSA, DPA and FOIA, please see Legal guidance and the useful links below:

MOJ Data Sharing and Protection Guidance –

http://www.justice.gov.uk/guidance/datasharing.htm

MOJ FOI Guidance - http://www.justice.gov.uk/guidance/guidancefoi.htm

Information Commissioner (DPA and FOI) - http://www.ico.gov.uk/

Civil Service Code and Management Code

1.9 Civil Servants are bound by the provisions of the Civil Service Code and the Civil Service Management Code, which specifically address the protection and handling of official information. Section 4.2 of the Civil Service Management code deals with 'Conduct: Confidentiality and Official Information'. A full copy of both codes can be found at: http://www.civilservice.gov.uk/iam/codes/index.asp.

Non-HMG assets (inc. commercial and personal data)

1.10 The GPMS is equally applicable to sensitive assets entrusted to HMG by others, such as foreign governments, international organisations, non-government organisations and private individuals. Whilst the GPMS is focused on the protection of assets related to National Security, it has been broadened out (at RESTRICTED and PROTECT) to include the protection of other types of non-national security related data. The introduction of PROTECT, as a purely non-national security related marking in January 2007 reflected the need to provide practical and flexible protection to data, such as, non-HMG, business, commercial, and personal data. PROTECT should not be sent to foreign governments or international organisations although it can be sent to industry as part of a classified contract provided the necessary contractual conditions are in

place. **[Redacted]**

International arrangements

1.11 Under specific reciprocal arrangements the GPMS is recognised by other designated friendly foreign governments. In these cases equivalent protections and markings ***must*** be recognised and applied (although it should be noted that the PROTECT, as a sub-national security marking, is not recognised under any of these current agreements). For details on applying GPMS in an overseas context and details of international security agreements - please see MR 10.

1.12 Where the GPMS is not recognised, either by a foreign country or a UK non-government organisation, and no other relevant agreements are in place, any sensitive assets received by HMG ***must*** be afforded the PROTECT marking as a minimum, although higher markings should be considered where appropriate.

The need-to-know principle

1.13 An underpinning principle to the GPMS and asset control is the so called 'need to know' principle. It is critical for the efficient running of government that information be shared to the right people at the right time. All staff have a responsibility to share information correctly and in a timely manner. This applies equally to protectively marked and non-protectively marked material. Regardless of the level of marking and or sensitivity of an asset, it must first be determined whether there is a legitimate business requirement for access or forward dissemination – does an individual or organisation actually require the information and for what ends? Will sharing support and be beneficial to Government/Departmental business? Of course it is not always easy to determine requirements without information being shared in first place and a judgement will need to be taken. However, the more sensitive the material, the more important it is to fully understand the requirements and ensure compliance with the necessary controls. It is never acceptable to grant casual access to protectively marked material. All staff (including contractors) handling or likely to handle, sensitive or protectively marked assets, ***must*** fully understand the need to know principle. 'The need to know principle accepts, in extremis, the need to share sensitive material to those without the necessary clearances, for example when immediate action is required to protect life or to stop a serious crime. In such circumstances a common sense approach should be

adopted, if time permits, alternatives should be considered and steps taken to protect the source of information.' If there is any doubt about providing access or onward dissemination of sensitive assets, individuals should consult their managers or security staff before doing so. Please also see section 5 Disclosure and other handling requirements.

Infringement and Breach Management

1.14 It is important that organisations clearly indicate to all staff the personal consequences expected should they be found responsible for the compromise of sensitive or protectively marked assets, be it deliberate or accidental. It should be made clear to those authorised to apply protective markings that it is an abuse of the system to use protective markings to protect against sensitivities that may be brought about by inefficiency or administrative error. Departments and Agencies ***must*** have a breach management system in place, which is complementary to their Human Resources/personnel/staff polices. Such a system should facilitate detection, ensure reporting and enable the correct disciplinary procedures to be enforced, and where necessary, to assist with any criminal proceedings. For further guidance please refer to Security Breach Management **[Redacted]**

2. Applying a protective marking

What can be protectively marked?

2.1 Applying a protective marking to an asset indicates the sensitivity, or Confidentiality (see 2.4 below), and thus the level of protection required. In principle protective markings could be applied to any HMG, or HMG handled, asset. However, it may be impractical to indicate the protective marking on the asset itself, such as equipment or even a building or room. Moreover, where an asset has inherent transferable value, or the nature of the item dictates the need for special handling, for example cash, firearms, dangerous substances, etc. it will probably require a greater level of protection than a marking may warrant, and may in some cases have quite separate statutory protections that ***must*** apply. Assets can be placed in containers that can be protectively marked, although they may attract unnecessary and unwanted attention and common sense judgements will always be required. However, where sensitive or valuable assets cannot be marked, relevant staff ***must*** be made aware of the protection and procedures required.

2.2 The guidance given here relates more readily to information assets; those produced and stored in formats such as paper, electronic/digital, magnetic and optical media and microform. However, the GPMS can apply equally to other types of sensitive or valuable assets, such as, equipment, hardware and valuables, or any indeed any government asset. Where assets are not protectively marked, but are otherwise sensitive or of particular value, Departments and Agencies ***must*** ensure that the appropriate, and in some cases that statutory controls (e.g. firearms, toxic/atomic materials, etc) are in place to protect them against compromise, loss or damage.

Determining the correct level

2.3 Applying the appropriate marking can be critical to effective business operations - too high a marking will lead to unnecessary, restrictive and expensive controls, which may deny access to those who have a real business requirement, or need to know. Conversely, applying too low a marking will put assets at risk of compromise, since

appropriate security controls may not be in place. Definitions for each level are found at Annex B.

The 'consequence of compromise'

2.4 In order to determine which marking is appropriate for the protection of an asset, the 'consequence of compromise' must be considered, to determine the asset value, and therefore the necessary controls and the protective marking. When assessing the value of an asset it will be necessary to consider the direct and indirect consequences of compromise in relation to a breach or loss of:

- **CONFIDENTIALITY:** The restriction of information and assets to authorised individuals.
- **INTEGRITY:** The maintenance of information systems and physical assets in their complete and proper form.
- **AVAILABILITY:** The continuous or timely access to information, systems or physical assets by authorised individuals.

A list of possible 'consequences of compromise' which would merit the usage of each protective marking as contained within the definitions at each level of marking are at Annex B**.** If any *one* of the consequences indicated within the definitions are possible, then the asset ***must*** be marked in line with this marking.

Valuing information assets: Confidentiality, Integrity and Availability

2.5**[Redacted]**

2.6**[Redacted]**

Summary of Availability and Integrity policy

2.7**[Redacted]**

Aggregation and accumulation

2.8 When protectively marked material is added to a file/folder, either paper or electronic, that file/folder ***must*** immediately attract the same marking of the highest protectively marked document/data within that file – for example if a RESTRICTED letter is added to a file of non-protectively marked material the file cover ***must*** be reclassified as RESTRICTED. The same principle should apply to any storage facility holding protectively marked material and any ICT system carrying protectively marked material ***must*** be accredited accordingly. Electronic Document Record Management systems (EDRM) are often able to 'lock-down' and restrict access at the individual document/paper level. In these cases there would be no need to protectively mark an entire electronic folder, but it should be noted that there may be sensitivity issues regarding the accessibility to the title of a document, which may in itself be classified. As a general principle electronic systems must afford the same level of protection and control to that of paper systems and adhere to the need to know principle. EDRM, or other electronic separation mechanisms, ***must*** be assessed as part of the accreditation process to ensure efficacy and assurance that the required levels of protection are met.

2.9 Aggregation and accumulation of data within ICT systems and on removable media is a more complex issue that needs careful consideration. The compromise of a mass of unclassified data, particularly one involving personal details, is likely to have a bigger impact and cause greater damage than the loss of one piece of unclassified data, and thus an adjustment to the impact level, but not necessarily the protective marking, may be required. It should be noted here that the concept of data dilution (i.e. the calculation that a small amount of classified data is somehow protected by the anonymity provided when stored within a mass of unclassified data) does not apply. However, it may not be appropriate to protectively mark each individual record within say a database, or indeed to classify the database as a whole. Departments ***must*** consider additional protective controls when looking at aggregated storage, control and transfer of data within ICT systems and on removable media. Whilst there is no absolute formula that can be applied with regard to protection of aggregated or mass data because of the complexities associated with the inter-connectively of data and systems, for example within Shared Services environments, **[Redacted]**

Valuing physical assets (people, buildings and sites)

2.10 When considering a loss of CONFIDENTIALITY, in so far as physical assets are concerned, for example items of equipment, it should be apparent which level of protective marking is appropriate –refer to definitions at Annex B and to mandatory requirements in the Security Policy No. 5 – Physical Security.

2.11 The loss of INTEGRITY or AVAILABILITY is more complex, as both direct and indirect consequences need to be considered. For example, the direct consequences of the theft of a personal computer may be limited as such equipment is relatively cheap and easy to replace, whereas the loss of information or software programmes stored in the computer, may have significant indirect consequences, particularly if back-up copies are not available.

2.12 Where it is appropriate, separate consideration should be given to the loss or interruption of an individual's function within an organisation, in so far as it might affect the efficiency of the organisation's business. It is clearly inappropriate to apply protective markings to employees, visitors, and members of the public. Their care and security should be safeguarded through the application of physical security measures in respect of the protection of buildings and sites, refer to Security Policy No. 5 – Physical Security and Security Policy No. 6 – Counter-Terrorism.

Marking an asset

2.13 When protectively marking an asset, typically a document, it must be clearly and conspicuously marked. It is considered good practice to mark each page at both the header and footer using bolded capital letters – for example **RESTRICTED**. File covers should be similarly marked. When marking e-mails it is best practice to put the marking in the subject or title box as well as in the message text, typically at the start or top of the e-mail.

Guidance on systems for control for protective markings

2.14 Departments and Agencies should make clear to managers that they are responsible for ensuring authorised individuals correctly mark sensitive assets. In support of this responsibility, organisations may wish to introduce controls and provide guidance on how to mark assets appropriately. Such controls may include:

a. restricting authority for deciding protective markings only to 'authorised' individuals,

b. minimising the use of high level protective markings, by restricting their application to senior managers and specific types of activity,

c. limiting assets requiring protective marking, for example, by encouraging the separation of the more sensitive information into appendices, so that the main body can be distributed more widely using less elaborate protective controls,

d. emphasising that documents should not necessarily be given the same marking as those to which they are attached, refer to or are in response to,

e. marking sections or individual paragraphs of a document separately to help individuals wishing to refer to information in the document to decide on an appropriate marking for that reference,

f. where possible, set time-expiry limits on markings so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release after a particular date, and is therefore only sensitive until it is published, such as official statistics

E-mail

2.15 The GPMS applies to e-mails in the same way as it does for any other data assets. However, e-mail as the main communication and information management tool within government, is worthy of special attention, highlighting some of the vulnerabilities inherent in this area.

2.16 **[Redacted]**

2.17 It is considered best practice to have an e-mail system that compels the user to select a protective marking, for example by use of a drop-down menu. When an e-mail system does not have this function, the marking should be clearly indicated in capitals within the subject box at the beginning of the title, - for example 'PROTECT: Personnel policy meeting' – by doing this the recipient can clearly see from their in-box the classification of the e-mail before they open it.

2.18 It is also good practice to put the protective marking within the e-mail text itself, again this should be completed in capitals and put at the top of the e-mail – this is to ensure that the marking appears should the e-mail be printed, or sent to an in-box that does not include the subject text.

2.19 E-mails are more often than not conversational documents, in other words they are added to by a number of different individuals in response to a query or question. It is therefore very important that individual recipients assess the entire contents of an e-mail 'string' before they add to it and forward it on – and as a result, assess the need for any additional protective marking. Unclassified e-mails may quickly become classified, as material is added or as new recipients are copied in. In some instances, particularly in an intelligence or military context, the names of the recipients may in itself require the e-mail to be protectively marked.

Descriptors

2.20 A descriptor is intended to re-enforce the 'need to know' principle by indicating the nature of an asset and the need to limit access. The application of a descriptor is only intended to highlight the need to take additional common sense precautions to limit access, the protective marking will take precedence and the asset must be handled accordingly. Descriptors should be clearly indicated, typically separated by a dash - for example **RESTRICTED – POLICY.** Cabinet Office maintains a list of core descriptors (see below) which all Departments and Agencies should use to describe the contents of protectively marked material where it is applicable. Departments and Agencies may devise their own descriptors and apply them to

information specific to their organisation, but are encouraged to use the core descriptors where they can. Where it is considered that such a descriptor may be of use by government generally, a request should be sent to the Cabinet Office Security Policy Division for it to be considered for inclusion in the Core Descriptor List. Descriptors do not generally indicate any special handling requirements above and beyond that already provided by the protective marking; although descriptors may indicate time sensitivity, for example BUDGET material may only be sensitive up to the Chancellor's budget announcement.

2.21 Descriptors should not be added to national security material being sent overseas as they are not recognised under any international agreements and are likely to cause confusion, unless there are previously agreed local arrangements.

Core Descriptor List

2.22

APPOINTMENTS: actual or potential appointments that have not yet been announced

BUDGET: Proposed or actual measures for the Budget before its announcement

COMMERCIAL: A commercial company's undertakings, processes or affairs

CONTRACTS: Tenders under consideration and the terms of tenders accepted

HONOURS: The actual or potential award of an Honour that has not yet been announced

INVESTIGATION: Investigations into disciplinary or criminal matters

LOCSEN: Locally sensitive information

MANAGEMENT: Concerning policy and planning affecting the interests of groups of employees

MEDICAL: Medical reports, records and related health material

PERSONAL: Material only to be seen by the addressee - this descriptor may be applied to non-protectively marked assets to limit access, in the first instance, to a named addressee - no other special handling is required.

PRIVATE, PERSONAL or PERSONAL DATA: Information collected through electronic Government services provided to the public and relating to the individual or an organisation: Access to be limited to the individual or organisation concerned and those representatives of agencies with a requirement for access under the governing legislation.

POLICY: Proposals on new or changed government policy before publication, or comment thereon

REGULATORY: Material which has come into the possession of government departments or agencies in the course of carrying out their statutory regulatory duties

STAFF: References to named or identifiable staff or personal confidences entrusted by staff to management

STATISTICS: information related to official statistics, often such information is only time sensitive and embargoed until general release or publication.

VISITS: Reference to future visits by, for example, royalty, Ministers or very senior personnel

"UK" Caveat

2.23 For material being sent, or likely to be sent overseas, the protectively marking should carry the 'UK' caveat in the following manner

It is important to note that the onus is on those sending material overseas to ensure that foreign Freedom of Information Legislation or other similar legislation does not result in the disclosure of UK protectively marked material, unless by agreement with HMG. Therefore the UK prefix and caveat should be used. The UK caveat should be

used within the UK if it is necessary to identify the source, or to differentiate it from other foreign protectively marked material. For full details of national caveats and sending material overseas please refer to International Protective Security Policy – MR 10.

Unclassified material

2.24 In some situations it is important that assets, particularly documents, are positively identified as non-sensitive or unclassified; for example in a military or intelligence environment. In this context the marking NON or NOT PROTECTIVELY MARKED is used. The term UNCLASSIFIED may also be used. Where there is no marking it should be assumed that the document is not protectively marked and should be handled accordingly. It is important to note that NON PROTECTIVELY MARKED or UNCLASSIFIED does not automatically equate to open access, in other words such material should not necessarily be published or posted on the internet or website.

Reclassifying assets

2.25 Only the originator can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied. Where the originating organisation has ceased to function, its successor becomes responsible. Where a successor cannot be traced, the holder of a copy document may change its marking only after consultation with all other addressees.

2.26 It is important that originators of protectively marked assets are made aware of the arrangements and controls which can be used to limit the official disclosure of sensitive information, including the possible release under the Freedom of Information Act or public release to the National Archives. Holders of protectively marked assets have the discretion to take into account local circumstances when selecting the most appropriate procedures and controls needed to provide an appropriate level of protection.

3. Handling – sending, storing and destruction

3.1 It is important to have an appropriate set of procedures for handling information assets, including:

a) copying
b) storage
c) transmission by post, fax, and e-mail/text messaging etc
d) transmission by spoken word, including mobile phone, voicemail, answering machines;
e) destruction

3.2 An effective system of control is essential for the protection of protectively marked and other valuable or sensitive assets. Such a system ***must*** allow all staff and contractors to know clearly:

a) what protectively marked documents they hold
b) what level of protection must be given
c) where it is held
d) who is authorised to see it of use it

and, at higher levels of protection

e) who has had access to it or has used it in the past

This should be achieve by applying the following baseline and discretionary controls relating to preparation, registration and filing, copying, custody, review, destruction, spot checks, electronic formats/and microform.

Preparation

3.3 Implementation of 'need to know' is the core of any good asset control system. The preparation of protectively marked assets must only be carried out by authorised individuals, who hold appropriate personnel security control and who have been properly briefed as to their security responsibilities.

Registering and filing

3.4**[Redacted]**

[Redacted]

[Redacted]

3.5 **[Redacted]**

3.6 **[Redacted]**

[Redacted]

3.7 **[Redacted]**

3.8 **[Redacted]**

3.9 **[Redacted]**

3.10 **[Redacted]**

3.11 **[Redacted]**

3.12 **[Redacted]**

3.13 **[Redacted]**

3.14 **[Redacted]**

3.15 **[Redacted]**

3.16 **[Redacted]**

3.17 **[Redacted]**

3.18 **[Redacted]**

3.19 **[Redacted]**

3.20**[Redacted]**

3.21 **[Redacted]**

3.22 **[Redacted]**

3.23 **[Redacted]**

3.24 **[Redacted]**

3.25 **[Redacted]**

3.26 **[Redacted]**

[Redacted]

3.27 **[Redacted]**

3.28 **[Redacted]**

3.29 **[Redacted]**

4. Special Handling of Protectively Marked material

4.1 This document should be read in conjunction with Security Policy No. 2 - Protective Marking and Asset control within the Security Policy Framework.

Special handling instructions

4.2 Applying a protective marking is the principle means of indicating an assets sensitivity and the requirements for its protection. Special handling instructions consist of additional markings which can be used in conjunction with a protective marking to reinforce application of the 'need to know' principle. In such cases the following special handling or additional markings may be applied:

- Descriptors
- Codewords
- Nicknames
- National caveats

For details on Descriptors, please refer to Security Policy No. 2 - Protective Marking and asset control.

4.3 **[Redacted]**

4.4 **[Redacted]**

4.5 **[Redacted]**

4.6 **[Redacted]**

4.7 **[Redacted]**

4.8 **[Redacted]**

4.9 **[Redacted]**

4.10 **[Redacted]**

[Redacted]

4.11**[Redacted]**

4.12 **[Redacted]**

4.13 **[Redacted]**

4.14 **[Redacted]**

4.15**[Redacted]**

[Redacted]

4.16 **[Redacted]**

4.17 **[Redacted]**

4.18 **[Redacted]**

4.19 **[Redacted]**

4.20 **[Redacted]**

4.21 **[Redacted]**

4.22**[Redacted]**

4.23 **[Redacted]**

Nicknames

4.24 A nickname comprises two words written in capital letters which may be used for administrative convenience in reference to a particular non-protectively marked asset or event where security is not required. Departments and agencies are responsible for selecting and assigning a nickname and for informing all concerned of its meaning.

[Redacted]

5. Carriage of Protectively marked assets

5.1 **[Redacted]**

5.2 **[Redacted]**

[Redacted]

5.3**[Redacted]**

[Redacted]

[Redacted]

5.4 **[Redacted]**

5.5 **[Redacted]**

[Redacted]

5.6 **[Redacted]**

5.7 **[Redacted]**

[Redacted]

5.8 **[Redacted]**

5.9 **[Redacted]**

5.10 **[Redacted]**

[Redacted]

[Redacted]

5.11 **[Redacted]**

5.12**[Redacted]**

5.13 **[Redacted]**

5.14 **[Redacted]**

5.15 **[Redacted]**

5.16 **[Redacted]**

5.17 **[Redacted]**

5.18 **[Redacted]**

5.19 **[Redacted]**

5.20 **[Redacted]**

5.21 **[Redacted]**

[Redacted]

5.22 **[Redacted]**

[Redacted]

5.23 **[Redacted]**

[Redacted]

5.24 **[Redacted]**

5.25 **[Redacted]**

5.26 **[Redacted]**

5.27 **[Redacted]**

5.28 **[Redacted]**

[Redacted]

5.29 **[Redacted]**

5.30 **[Redacted]**

5.31 **[Redacted]**

[Redacted]

[Redacted]

[Redacted]

5.32 **[Redacted]**

6. Disclosure and other handling requirements

Disclosure of protectively marked assets

6.1 Under some circumstances protectively marked material may need to be disclosed to those without the proper authority. In extremis, for example, where lives are at stake or a where a criminal act might be imminent, it may be clearly necessary to share the contents of protectively marked material to those without the proper authority, in order that immediate preventative action maybe taken. In such circumstances, where it is possible and expedient to do so, only the information required to take the necessary action should be released.

6.2 Under Freedom of Information Legislation protectively marked material may be released. Requests for such information under FOI should be considered in much the same way as any other requests, although any material that has national security implications or comes directly or indirectly from bodies or organisations dealing with security matters ***must*** in the first instance be referred to the Ministry of Justice Clearing House (clearinghouse@justice.gsi.gov.uk; 0207210 8986). **[Redacted]**

6.3 The Public Records Act 1958 and 1967 also requires that public records with a research or historical content should be transferred to the National Archives for public disclosure. This refers equally to protectively marked material, although security considerations will apply – please refer to your Departmental Records Officer or the National Archives (http://www.nationalarchives.gov.uk/recordsmanagement) direct.

6.4 Where protectively marked material is disclosed it is considered best practice to over-stamp the protective marking to indicate declassification – for example 'Released under FOI in full on [date]' or 'Released under Public Records Act [date]' or simply 'DECLASSIFIED on [date]'. Similarly, if material is covered by an FOI exemption or should not be disclosed under Data Protection legislation organisation may signal this by adding 'NOT FOR DISCLOSURE'. Organisations that receive and use information from the Security and Intelligence Agencies may also wish to annotate material to indicate confirmation of the application of Section 23 exemption under FOI, which is a absolute exemption applying to any material supplied by or related to a number of

specified (within the Act) organisations, including the Security and Intelligence Agencies.

6.5 For further details of disclosure in over overseas context see International Protective Security Policy – MR 10 and UK caveat.

Interdepartmental committees

6.6 Departments and Agencies, when setting up a committee, advisory panel or similar body made up in whole or in part of non-government employees, must ensure that government assets, whether or not

protectively marked, are protected by appropriate security arrangements. This responsibility does not rest upon other departments or agencies which may have subsequent dealings with the committee or body concerned.

6.7 Instructions must make it clear that if individuals who are employed outside government, are to be associated in any way with work involving access to protectively marked assets, the DSO of the department responsible for the committee must be consulted. It is the DSO's responsibility to determine what security arrangements are necessary before any such material can be passed.

6.8 The Secretary of the committee or group which is involved in handling protectively marked assets should normally be a government employee working on government premises, and consequently able to accept responsibility for safeguarding the protectively marked assets involved. Only in exceptional circumstances should a non-government official be appointed as Secretary. Where highly technical subjects are involved, it may not be possible to appoint a government employee as secretary. In such cases, this difficulty may be overcome by appointing a non government and a government employee as Joint Secretaries. This will allow the government employee to handle the committee's or group's protectively marked assets. In so far as security arrangements are concerned, non officials should be treated as far as possible in the same way as consultants.

Parliamentary select committees

6.9 General guidance for officials giving oral or written evidence to Parliamentary Select Committees is contained in the booklet *Departmental Evidence and Response to Select Committees* published by the Cabinet Office. In the case of such committees, it is often difficult to decide what protectively marked information can properly be withheld rather than what can be disclosed. Protectively marked memoranda, or annexes to memoranda, and the full transcripts of oral evidence containing protectively marked information, are made available to members (and committee staff) during Committee or Sub Committee meetings and, on request, in the Committee Office. Members may not take protectively marked documentation away with them.

6.10 The House of Commons authorities are responsible for ensuring that information protectively marked SECRET or TOP SECRET to be disclosed to the Select Committees (and committee staff where necessary) will be limited to those individuals to whom the issuing department or agency has agreed to release it. In practice this would mean only the members of the Committee or Sub Committee concerned and, in the case of a Sub Committee, also the main Committee Chairman. The release of information protectively marked TOP SECRET to members of Select Committees is subject to the approval of the responsible Minister in each case.

6.11 The disclosure of information marked RESTRICTED or CONFIDENTIAL will be similarly limited, except that where it has been disclosed to Sub Committee members it may also be made available to the main Committee members. Notwithstanding the restrictions imposed protectively marked information may be disclosed to Specialist Advisers to Select Committees, provided they hold appropriate security clearances in accordance with arrangements agreed with the Clerk of the House.

6.12 Where evidence has been given in a closed session, the witness should, at the end of the session, let the Clerk know which parts of the evidence are sensitive. Pending the Committee's final decision on what they will agree to omit from the published version, the Clerk will instruct the shorthand writer not to send for printing the transcript of these passages but will send two copies of the full transcript to the department. One copy is for retention, the other for return to the Clerk with those passages side lined

which contain sensitive information which, in the department's judgement, it would not be in the public interest to publish.

6.13 One copy of the full transcript is also retained in the Committee Office, where appropriate personnel and physical security controls are in place, for Committee Members who are authorised to have access to it.

Elected representatives on local authorities

6.14 During the course of discussions between departments and local authorities it may be necessary to disclose protectively marked information. Care should be taken on these occasions to ensure that the non departmental recipients are aware of their responsibilities for the protection of such material, hold appropriate security clearance and that access is limited to those individuals with a genuine 'need to know'.

6.15 The 'need to know' principle applies in particular to elected representatives on local authorities or their associations, as they are liable to frequent change. The safest course is to impart only the minimum information required to achieve the particular purpose and then only to individuals who are known and trusted, and preferably to officials, because of their permanency.

6.16 When consulting such outside bodies, departments should first approach senior officials and discuss with them how far the protectively marked information will need to be circulated in the local authority. This should be kept to a minimum and, wherever possible, discussions relating to a topic which, in total, requires a high level of protection should be undertaken at the lowest possible level of protective marking.

ANNEX A

Universal baseline controls for protectively marked material

1. The following baseline controls ***must*** be universally applied at all levels of protectively marked material:

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

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

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

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

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

f) A file, or group of protectively marked documents or assets, must carry the highest marking contained within it (for example a file or e-mail string containing CONFIDENTIAL and RESTRICTED material must be covered by the higher marking (e.g. CONFIDENTIAL).

ANNEX B

Definitions of protective markings

[Redacted]

PROTECT	
Asset Value - consequence of compromise	**The compromise of assets marked PROTECT would be likely to:** • Cause distress to individuals (section 38*) • Breach proper undertakings to maintain the confidence of information provided by third parties (sections 41, 43*) • Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and or/the e-government Security Framework). (section 44*) **And, depending on the severity of the circumstances:** • Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies (section 43*) • Prejudice the investigation or facilitate the commission of crime (sections 30, 31*) • Disadvantage government in commercial or policy negotiations with others (sections 43, 35, 36*)
Level of protection	**The level of protection provided for assets marked PROTECT should ensure that users:** • promote discretion in order to avoid unauthorised access.
Baseline objectives – Disposal and destruction	**The baseline security objectives for PROTECT are:** • Handle, use, and transmit with care • Take basic precautions against accidental compromise or opportunist attack • Dispose of or destroy in a manner to make reconstruction unlikely.
Access requirements	• Other than 'need to know' principle, no specific national security clearance is required.
Descriptors	Where possible a descriptor should be used with PROTECT. Descriptors associated with PROTECT include: APPOINTMENTS, COMMERCIAL, PERSONAL DATA, CONTRACTS, HONOURS, INVESTIGATION, LOCSEN, MANAGEMENT, MEDICAL, PRIVATE, REGULATORY, STAFF.
Telephone	**[Redacted]**

Email	**[Redacted]**

.

NB - PROTECT is not a National Security classification and its purpose is to delineate a stratum of official information which needs to be protected from compromise but for which the measures required to safeguard National Security information at RESTRICTED are considered disproportionate. PROTECT can be applied to any information which requires Confidentiality at Impact Level 1 or 2, therefore it is essential that a risk assessment is undertaken to determine the impact level (1 or 2) to handle accordingly. Due to wide range of official information that can be marked PROTECT the marking should where possible be accompanied by a descriptor e.g. 'PROTECT – COMMERCIAL', 'PROTECT – PERSONAL DATA' etc. **[Redacted]**

3.

RESTRICTED	
Asset Value - consequence of compromise	The compromise of assets marked **RESTRICTED** would be likely to: • adversely affect diplomatic relations *(section 27*)* • cause substantial distress to individuals *(section 38*)* • make it more difficult to maintain the operational effectiveness or security of UK or allied forces *(sections 26,27*)* • cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies *(section 43*)* • prejudice the investigation or facilitate the commission of crime *(sections 30, 31*)* • breach proper undertakings to maintain the confidence of information provided by third parties *(sections 41, 43*)* • impede the effective development or operation of government policies *(sections 35,36*)* • breach statutory restrictions on the disclosure of information (except the Data Protection Act - which can be addressed by other impact statements and/or the e-Government Security Framework). *(section 44*)* • disadvantage government in commercial or policy negotiations with others *(sections 43, 35,36*)* • undermine the proper management of the public sector and its operations *(sections 35, 36*)*
Level of protection	**[Redacted]**
Baseline objectives – Storage and	**[Redacted]**

control	
Access requirements	**[Redacted]**
Application requirements	**[Redacted]**
Telephone	**[Redacted]**

[Redacted]

4.

CONFIDENTIAL	
Asset Value - consequence of compromise	The compromise of assets marked **CONFIDENTIAL** would be likely to: • materially damage diplomatic relations, that is, cause formal protest or other sanctions *(section 27*)* • prejudice individual security or liberty *(section 38*)* • cause serious damage to the operational effectiveness or security of UK or allied forces *(section 26, 27*)* • cause serious damage to the effectiveness of valuable security or intelligence operations *(sections 23, 24*)* • work substantially against national finances or economic and commercial interests *(section 29*)* • substantially undermine the financial viability of major organisations *(section 43*)* • impede the investigation or facilitate the commission of serious crime *(sections 30, 31*)* • seriously impede the development or operation of major government policies *(sections 35, 36*)* • shut down or otherwise substantially disrupt significant national operations *(section 24*)*
Level of protection	**[Redacted]**
Baseline objectives – Storage and control	**[Redacted]**
Baseline objectives – Disposal and	**[Redacted]**

destruction	
Access requirements	**[Redacted]**
Application requirements	**[Redacted]**

5.

SECRET	
Asset Value - consequence of compromise	The compromise of assets marked **SECRET** would be likely to: • raise international tension *(sections 27, 24*)* • seriously damage relations with friendly governments *(section 27*)* • threaten life directly or seriously prejudice public order or individual security or liberty *(sections 38, 24*)* • cause serious damage to the operational effectiveness or security of UK or allied forces *(sections 24, 26, 27)* • cause serious damage to the continuing effectiveness of highly valuable security or intelligence operations *(sections 23, 24*)* • cause substantial material damage to national finances or economic and commercial interests *(section 29*)*
Level of protection	**[Redacted]**
Baseline objectives – storage and control	**[Redacted]**
Baseline objectives – Disposal and destruction	**[Redacted]**
Access requirements	**[Redacted]**
Application requirements	**[Redacted]**

6.

TOP SECRET	
Asset Value - consequence of compromise	The compromise of assets marked **TOP SECRET** would be likely to: • threaten directly the internal stability of the UK or friendly countries *(section 24*)* • lead directly to widespread loss of life *(section 38*)* • cause exceptionally grave damage to the effectiveness or security of UK or allied forces *(sections 24, 26, 27*)* • cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations *(sections 23, 24*)* • cause exceptionally grave damage to relations with friendly governments *(section 27*)* • cause severe long term damage to the UK economy *(section 29*)*
Level of protection	**[Redacted]**
Baseline objectives – storage and control	**[Redacted]**
Baseline objectives – Disposal and destructions	**[Redacted]**
Access requirements	**[Redacted]**
Application requirements	**[Redacted]**

ANNEX C - [Redacted]

Appendix 1 - [Redacted]

Annex D

Procedures for transporting bulky protectively marked assets

1. The following procedures specify the required security standards to be applied when bulky assets protectively marked up to and including SECRET are moved within the UK and overseas.

2. In the case of assets protectively marked TOP SECRET, specific prior approval for transit ***must*** be sought from the departmental security branch. The referral should include a proposed Security Plan.

3. The carriage of bulky 'classified' NATO assets is separately covered in the following regulations:

- ***NATO - North Atlantic Treaty Organisation - CM(55)15(Final)*** **and** ***The Supplement***

[Redacted]

4. The following definitions are used in the transportation of bulky sensitive assets:

Authority	The department or agency responsible for the security of the assets.
Consignor	The contractor, department or agency or other organisation responsible for initiating the transport of the assets to the consignee.
Consignee	The contractor, department or other organisation which is the ultimate recipient of the assets.
Container	A receptacle of robust construction with or without lockable opening.
Crate	A container or open or slatted construction
Locker	Secured by an approved security lock
Asset	Equipment and components but not documents
Movement	An approved carrier or agent acting on behalf of the consignor - in certain circumstances the consignor will also act as the

documents	shipper.
Shipper	An approved carrier or agent acting on behalf of the consignor - in certain circumstances the consignor will also act as the shipper.

5. When the movement of assets is subject to contract, the contract should stipulate the point at which the ownership of the assets changes. Unless the contract provides otherwise, the responsibility for the secure transport of the assets should change at the same time as the ownership. The Authority is responsible for approving arrangements for the secure movement of bulky protectively marked assets.

Method of movement

[Redacted]

7. The consignor must be satisfied that all relevant matters such as storage in transit, supervision of loading and unloading, and the procedures to be adopted in the event of an accident, breakdown, diversion etc are included in the Security Plan**.** Where the consignor is not the Authority, the consignor must obtain the Authority's approval to the Method of Movement Plan**,** prior to the movement of the assets**.**

8. **[Redacted]**

Notice of movement

9. **[Redacted]**

10. **[Redacted]**

11. **[Redacted]**

Physical security controls

12. The physical security controls to protect protectively marked assets in transit will vary according to the level of marking, the nature, substance and size, the itinerary and means of transport. A consignment should be given the level of protection commensurate to the highest protectively marked component involved. When a bulky protectively marked asset is being moved the Authority, in conjunction with the consignor, should consider if handling

could be simplified by the removal and separate transmission of any detachable protectively marked component.

13. **[Redacted]**

14. **[Redacted]**

15**. [Redacted]**

Method of transport

16. **[Redacted]**

[Redacted]

17.**[Redacted]**

18. **[Redacted]**

19. **[Redacted]**

Appendix 1 - [Redacted]

Annex E - [Redacted]

Personnel Security

Introduction

1. This section is designed to help those with security responsibilities identify appropriate levels of assurance for all employees and security clearances for those requiring access to sensitive government information and other important or valuable assets. The current policy for Personnel Security Vetting, which came into effect on 1 January 1995, was set out in a statement made by the Prime Minister, on 15 December 1994 - refer to Appendix 1. The statement includes reference to the framework of personnel security controls that are applied to individual's who, in the course of their work, have access to, or knowledge or custody of, sensitive government information or other valuable assets. It also provides guidelines for line managers as to their responsibilities for personnel security.

'Need to know'

2. The dissemination of sensitive information and assets should be no wider than is necessary for the efficient conduct of an organisation's business and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. This 'need to know' principle is fundamental to the protection of sensitive government assets. It applies both within a department or agency and when dealing with individuals outside of it.

3. Departments and agencies must ensure that employees are made fully aware of their personal responsibility to apply the 'need to know' principle within their own area of activity. They should be instructed that if there is any doubt about giving access to sensitive assets to other individuals, or organisations, before doing so, they should consult their line manager or a member of the organisation's security staff.

Heads of Departments and Special Advisers

4. The Head of the Home Civil Service is responsible for carrying out the vetting and subsequent review of security clearances for Permanent Secretary Heads of Government Departments. The appropriate Head of Department should discuss, with

the Minister concerned, the need for, and level of clearance required by, Special Advisers to Ministers, both inside and outside the Cabinet.

Management responsibilities

5. Managers at the more senior levels of the management chain should be given specific responsibility for ensuring that:

   a. All individuals working in posts involving access to, or knowledge or custody of, sensitive government assets, have appropriate levels of assurance and security clearance.

   b. When security clearances are reviewed, or when post holders change, line managers are consulted as to whether or not there is a continuing need for the posts to attract levels of assurance or security clearances, and if so, the controls required.

6. Security vetting does not, on its own, provide a guarantee of an individual's integrity and trustworthiness. Since individuals and their circumstances change, a security clearance is only as good as the background records and other investigations on which it is based at the time the process is carried out. It is important that personnel security continues after the initial security clearance is approved and that any new information or concerns that may affect the reliability of a person are brought promptly to the attention of the appropriate authorities. This is achieved through a combination of aftercare and security clearance review procedures.

Line management responsibilities

7. Effective personnel security is dependent on the support of line managers. This applies equally in industry and government. It is important that government departments and agencies, and List X contractors and sub-contractors, stress to their line managers that security is an on-going management responsibility. It should be made clear that they are responsible for:

a. Maintaining the standards of security expected.

b. Briefing post holders about the protection of assets and processes under their control.

8. In particular, they should be on the look out for potential difficulties or conflicts of interests among staff and, where identified, report any concerns as soon as possible to the appropriate authority. For further details about line management's responsibilities for personnel security see, the Line Manager's Guide – Appendix 8.

Personnel branch responsibilities

9. Effective personnel security controls also require close cooperation between the personnel (including welfare) and security branches to ensure that:

a. Personnel branches are reminded from time to time of issues likely to be of security significance, for example, Departmental Security Officers (DSOs) should bring the Baseline Standard (BS) procedures to the attention of those in their organisation responsible for personnel recruitment.

b. Information likely to be of security significance is routinely passed to the security branch and checks are carried out to ensure that no relevant information has been overlooked.

c. The security branch is consulted about an individual with Counter-Terrorist Check (CTC), Security Check (SC) or Developed Vetting (DV) clearance, for whom security concerns have been raised, before the individual is transferred to another CTC, SC or DV post.

Assessment of security clearance levels

10. Before initiating the security vetting process for a security clearance, departments, agencies and List X contractors should review the need for, and level of, security clearance required to fulfil the duties of the post. Please see the Government Protective Marking System and Asset Control section for details of appropriate levels of security clearance. Further advice should be sought from the DSO or, in the case of List X contractors, the Security Adviser or Contracting Authority.

11. To use the assessment guide effectively requires a clear understanding of the protective marking system and a good knowledge of the types and levels of assets that an individual will need access to, or knowledge or custody of, when working in a particular post.

Assessing the levels of assurance required

12. To ensure that the appropriate level of assurance is achieved, departments, agencies and List X contractors should:

    a. Involve line managers in identifying sensitive posts.

    b. Keep such posts to a minimum and ensure that the level of assurance is appropriate.

    c. Apply the same criteria to non-List X contractors and consultants, and List X sub-contractors.

    d. Ensure that all posts **[Redacted]** are covered by the ***Security Service Act 1989*** **[Redacted]**

    e. Ensure that posts requiring access to sensitive assets belonging to another country or international organisation are subject to appropriate security clearances. For further details see, the International Protective Security policy section (MR 10).

13. Regardless of the individual's position, grade or role in an organisation, and whether temporary or permanent, it is the work of the post and the degree of access to sensitive government assets that indicates whether or not the BS or security clearance is required. In some cases, the future career prospects of an individual, rather than the work of a post, may indicate a need to consider a security clearance.

14. **[Redacted]**

Personnel security controls

15. Four levels of personnel security controls are available depending on the level of assurance required:

- **Baseline Standard (BS) -** please refer to the Baseline Personnel Security Standard (see MR 23)
- **Counter-Terrorist Check (CTC) -** refer to paragraph 19
- **Security Check (SC) -** refer to paragraph 20
- **Developed Vetting (DV) -** refer to paragraph 21

16. Of these CTC, SC and DV are formal security clearances obtained through the security vetting procedures, set out later in this section. The BS is not a security clearance but aims to provide an appropriate level of assurance as to the trustworthiness and integrity of individuals handling sensitive government assets. In some cases a BS may need to be reinforced with some of the checks used in formal security clearances. Once approved, clearances are monitored and reviewed at regular intervals.

Baseline controls

17. In so far as the protection of assets is concerned, the security controls adopted by departments, agencies and List X contractors must always meet the following Personnel Security Baseline Objectives:

- **RESTRICTED:** Other than the 'need to know' principle, no specific security measures required - In some cases a CTC may need to be considered.

- **CONFIDENTIAL:** BS - In some cases a CTC or certain elements of an SC may also be required.

- **SECRET:** SC - In some cases a BS may be sufficient - Some components of the SC will not be relevant to every post. In many cases, government departments and agencies will wish to conduct all these checks; but there is discretion to dispense with those not relevant to the needs of the post. **[Redacted]**

- **TOP SECRET:** DV - In some cases an SC may be sufficient.

Baseline Standard (BS)

18. For guidance on the procedures for the Baseline Standard – please refer to the Baseline Personnel Security Standard (see MR 23)

Counter-Terrorist Check (CTC)

19. A CTC clearance is required for individuals who are to be employed in posts which:

    a. Involve proximity to public figures who are assessed to be at particular risk from terrorist attack.

    b. Give access to information or material assessed to be of value to terrorists.

    c. Involve unescorted access to certain military, civil, industrial and commercial establishments assessed to be at risk from terrorist attack.

A CTC, alone, does not allow an individual access to, or knowledge or custody of, protectively marked assets. For guidance on the vetting procedures for obtaining a CTC clearance - refer to paragraph 28.

Security Check (SC)

20. An SC clearance is required for those individuals who are to be employed in posts which:

    a. Require individuals to have long-term, frequent and uncontrolled access to SECRET assets.

    b. Require individuals to have occasional, supervised access to TOP SECRET assets **[Redacted]**

    And for individuals who:

    c. While not in such posts, will be in a position to directly or indirectly bring about the same degree of damage.

    d. Will have sufficient knowledge to obtain a comprehensive picture of a SECRET plan, policy or project.

    e. Are being considered for employment where it would not be possible to make reasonable career progress without security clearance for access to SECRET assets.

f. Need access to certain levels of protectively marked material originating from another country or international organisation – refer to the International Protective Security policy section.

21. An SC clearance should not usually be required for:

a. Occasional access to SECRET assets in the normal course of business or during conferences or courses.

b. Custody of a small quantity of SECRET assets.

c. Entry to an area where SECRET assets are stored.

d. Work in areas where SECRET or TOP SECRET information might be overheard.

e. Use of equipment capable of handling SECRET information, provided that access controls are in place.

22. In the above circumstances, a BS - please refer to the Baseline Personnel Security Standard (see MR 23) - should usually be sufficient. For guidance on the vetting procedures for obtaining an SC clearance - refer to paragraph 33.

Developed Vetting (DV)

23. A DV clearance is required for those individuals to be employed in posts where:

a. The post holder requires frequent, uncontrolled access to assets protectively marked TOP SECRET, **[Redacted]**

b. The post holder, while not in such a post, will be in a position to, directly or indirectly, bring about the same degree of damage, for example:

i. Threaten directly the internal stability of the UK or friendly nations;

ii. Cause exceptionally grave damage to relations with friendly nations;

iii. Lead directly to widespread loss of life;

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

v. Cause exceptionally grave damage to the effectiveness or security of UK or allied forces; and/or

vi. Cause severe long-term damage to the UK economy.

c. The post holder requires frequent, uncontrolled access to Category I nuclear material.

d. The post holder requires access to certain levels of protectively marked material originating from another country or international organisation.

24. **[Redacted]** A DV clearance should not usually be required for:

- Occasional, supervised access to limited quantities of TOP SECRET assets in the normal course of business or during conferences or courses.

- Custody of a small quantity of TOP SECRET assets.

- Entry to areas where TOP SECRET assets are stored.

- Work in areas where TOP SECRET information might be overheard.

- Use of equipment capable of handling TOP SECRET information, provided that access controls are in place.

- **[Redacted]**

- For police officers in posts where there is a threat from Serious or Organised Crime, SC Clearance is sufficient provided wider local checks are carried out in the form of Police Management Vetting (MV). In such posts, ongoing management of the clearance should be augmented by the use of the Annual Security Appraisal Form (SAF).

25. In the above circumstances an SC clearance - refer to paragraph 33 - should be sufficient. For guidance on the vetting procedures for obtaining a DV clearance - refer to paragraph 38.

Procedures for security clearance

26. Obtaining security clearances is expensive and time consuming. Before proceeding, confirm that the individual's requirement for security clearance is appropriate to the needs of the post. Depending on the level of access needed, and consequently the type of security clearance required, not all of the security vetting stages explained below may be relevant. Please refer to the Government Protective Marking System and Access control section for more details.

27. **[Redacted]**

Counter-Terrorist Check (CTC)

28. To carry out a CTC, departments, agencies and List X contractors must initiate the security vetting process set out below.

29. The following security vetting stages are mandatory before a CTC clearance can be approved:

- **Baseline Standard -** please refer to the Baseline Personnel Security Standard (see MR 23)
- **Departmental/Company Records Check -** refer to paragraph 54
- **Security Questionnaire -** refer to paragraph 61
- **Criminal Record Check -** refer to paragraph 77
- **[Redacted]**

30. When a DV or SC is being processed, the vetting procedures incorporate those stages used for a CTC; consequently there is no need to carry out a separate CTC.

31. On completion of, or during the vetting process as appropriate, the information collected should be assessed and a decision made to refuse or approve the individual a CTC clearance.

32. **[Redacted]**

Security Check (SC)

33. The following security vetting stages comprise a full SC clearance:

Baseline Standard - please refer to the Baseline Personnel Security Standard (see MR 23)

Departmental/Company Records Check - refer to paragraph 54

Security Questionnaire - refer to paragraph 61

Criminal Record Check - refer to paragraph 77

Credit Reference Check - refer to paragraph 101

[Redacted]

34. **[Redacted]**

35. To carry out an SC, departments, agencies and List X contractors must initiate the security vetting process set out below.

36. On completion of, or during the vetting process as appropriate, the information collected should be assessed and a decision made to refuse or approve the individual an SC clearance.

37. **[Redacted]**

Developed Vetting (DV)

38. The following security vetting stages are mandatory before a DV clearance can be approved:

Baseline Standard - please refer to the Baseline Personnel Security Standard (see MR 23)

Departmental/Company Records Check - refer to paragraph 54

Security Questionnaire and DV Supplement - refer to paragraph 61

Criminal Record Check - refer to paragraph 77

Credit Reference Check - refer to paragraph 101

[Redacted]

Review of personal finances - refer to paragraph 142

Subject Interview and further enquiries - refer to paragraph 147

39. To carry out a DV, departments, agencies and List X contractors must initiate the security vetting process set out below. Security Controllers must first seek authorisation for DV clearance from the Contracting Authority see, **Authorisation for DV Clearance in Industry** – refer to appendix 2.

40. On completion of, or during the vetting process as appropriate, the information collected should be assessed and a decision made to refuse or approve the individual a DV clearance.

Provisional clearance

41. Departments and agencies may allow an individual access to assets requiring DV clearance, before completion of the security vetting process, provided that the first stages, amounting to an SC, have been satisfactorily completed and, where possible, the Subject Interview stage has been carried out. In all cases, the remaining DV procedures should be completed as soon as possible.

For List X Contractors

42. Unless specially authorised by the Contracting Authority, provisional clearance does not apply for contractor employees.

Retention of security clearance documentation

43. It is important that departments, agencies and List X contractors, keep full and up to date personnel security records for all their employees who hold security clearances.

44. Departments and agencies should retain personnel security records for the minimum periods shown below, even after the individual ceases to be employed in government service. This applies equally where records are held on List X contractors working on government contracts:

    a. 5 years after the individual has retired at the normal retirement age.

    b. 10 years after the individual has retired or left before the normal retirement age, but not exceeding a period of 5 years after the normal retirement age.

    c. 1 year after the individual's death.

45. Personnel security records held in respect of List X and non-List X contractors and consultants should be retained for a minimum period of 1 year after the individual has left the company.

Security Questionnaires

46. Security Questionnaires are important documents. They contain a signed declaration by the individual confirming that they understand and agree to the vetting checks that are undertaken as part of the vetting process. The declaration could constitute important evidence in the event of any subsequent action connected with the security clearance (e.g. in relation to an investigation, an appeal or legal challenge). But the retention of all security questionnaires has to be weighed against other factors, for example, the likelihood of legal action, the level of security clearance and storage difficulties.

47. Department and agencies have discretion to destroy some questionnaires after retention for the following minimum periods:

    a. 6 months, where any security clearance is approved and an offer of appointment has been made, but the candidate has not taken up employment.

b. 6 months, for routine SC clearances, where the individual is employed.

c. 3 years, for any level of security clearance where applicants were refused security clearance and as a result were not employed.

48. In all cases of DV clearance, and where current employees' security clearance has been refused or withdrawn, security questionnaires must be retained with the individual's personnel security records for the minimum period.

49. List X contractors must retain security questionnaires in accordance with the requirements - refer to paragraph 45 - since they are generally the only record of security clearance.

Retention of Paper Records

50. Where security questionnaires are scanned and stored electronically, it is for departments and agencies to decide whether their storage and retrieval system is sufficiently reliable and robust for them not to retain paper versions as well for the prescribed periods.

Audit and Assurance for National Security Vetting

51. Departmental Security Units (DSUs) should carry out an audit of personnel security as part of their annual report to the Head of Department. This will reduce the effort required to perform audit by incorporating it into an existing process **[Redacted]**

Vetting statistics

52. Departments and agencies must maintain an up to date record of the following statistics:

a. The number of posts in the organisation requiring CTC, SC and DV clearances.

b. The number of CTC, SC and DV clearances and reviews carried out annually.

c. The number of security clearance refusals and withdrawals made annually, and the number of appeals that have resulted.

Where possible, figures for contractors should be recorded separately.

Security Vetting Stages

Stage 1 - Baseline Standard (BS)

53. Confirm that the BS has been approved for the individual. If not, carry out the BS - please refer to the Baseline Personnel Security Standard (see MR 23) then proceed to the next stage - Departmental/Company Records Check. Ideally, no National Security Vetting (NSV) checks should be carried out until the Baseline Standard has been met in full. Where this is not practicable, NSV checks may be carried out once the subject's identity has been satisfactorily confirmed. The remaining baseline checks should be carried out as soon as possible thereafter. If the subject is not properly identified then any further checks are meaningless.

Stage 2 - Departmental/Company Records Check

54. Departmental or company records should provide a significant amount of relevant information about the individual, for example, from personal files, staff reports, sick leave returns and security records.

55. A check of these records should highlight any obvious areas of the individual's behaviour or circumstances which might indicate the need for careful consideration. This stage of the security clearance process involves:

    a. Checking departmental or company records.

    b. **[Redacted]**

    c. Checking the individual's residence history.

56. Whenever possible a check of departmental or company records should be completed without the knowledge of the individual. This is particularly important for existing employees, as sensitive handling of a refusal to approve security clearance at an early stage, may prevent later difficulties.

[Redacted]

57. **[Redacted]**

[Redacted]

58. **[Redacted]**

    [Redacted]

    [Redacted]

    [Redacted]

59. **[Redacted]**

60. To continue with the vetting or review process, proceed to the Security Questionnaire stage.

Stage 3 - Security Questionnaire

For government departments and agencies

61. When asking the individual to complete the Security Questionnaire, the individual should be:

    a. Informed of the level of security clearance being sought, or the need for the review.

    b. Reminded to read, in particular, the government's vetting policy statement on Page 2.

    c. Asked to answer all questions, except those on Page 12.

    d. Asked not detach the tear off section on Page 7.

For List X contractors

62. When asking the individual to complete the Security Questionnaire, the individual should:

    a. Be informed of the level of security clearance being sought, or the need for the review.

    b. Be reminded to read, in particular, the government's vetting policy statement on Page 2.

c. Be asked to answer all questions, except those on Page 12.

d. Be informed of the right to withhold, from the contractor or sub-contractor, the contents of the criminal declaration, questions 33 and 34 on Page 7. On completion, the individual should sign, date and detach the tear off section, place it in an envelope provided, seal and sign across the flap and attached it firmly to the front of the Security Questionnaire.

63. **[Redacted]**

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

[Redacted]

[Redacted]

64. **[Redacted]**

65. **[Redacted]**

[Redacted]

66. **[Redacted]**

67. **[Redacted]**

[Redacted]

68. **[Redacted]**

[Redacted]

69. **[Redacted]**

70. **[Redacted]**

For DV clearance

71. **[Redacted]**

72. Send the completed Security Questionnaire with the sealed envelope, containing the Criminal Declaration attached and the DV Supplement, or DV Supplement (Review), to the Contracting Authority.

73. The Contracting Authority will assume responsibility for the remainder of the security clearance process.

74. The Contracting Authority will advise the List X contractor of its decision. Further discussions between the contractor, Contracting Authority and Security Adviser, may be necessary to resolve how to manage any potential problem that may arise from a refusal of security clearance.

75. For specific guidance and recommendations concerning assessment see, ***Assessment of Vetting Information -*** refer to paragraph 165***.***

76. To continue with the vetting or review process, proceed to the Criminal Record Check stage.

[Redacted]

77. **[Redacted]**

78. **[Redacted]**

[Redacted]

79. **[Redacted]**

80. **[Redacted]**

81. **[Redacted]**

82. **[Redacted]**

83. In cases where there are doubts about the individual's identity or nature of convictions, it may be necessary to seek further information from the individual.

For DV clearance

84. Departments and agencies should ask the NIS for criminal records on:

    a. The individual

    b. The individual's spouse or partner

    c. The individual's parents, step parents or guardians

    d. Where the individual is under 21 years old, brothers and sisters who live with them in their family home.

NIS response

85. In response to a request for a Criminal Record Check, the National Identification Service (NIS) will provide details of any convictions recorded or stamp the form 'No Trace in NIS on Particulars Given'.

86. Where further information is required about a conviction, a copy of the Security Questionnaire should be sent to the NIS with a covering letter. The NIS will make the appropriate enquiries with the relevant police force and return the questionnaire with the results of the enquiries.

Spent convictions

87. Under the provisions of the ***Rehabilitation of Offenders Act 1974*** certain convictions are deemed to be 'spent' after a given period of time if an offender remains free of conviction during that period. The following are exceptions to this rule:

    a. Life imprisonment

    b. Imprisonment or corrective training for longer than 30 months

    c. Preventive detention

    d. Detention during Her Majesty's pleasure or for life, or for longer than 30 months, passed under the ***Children and Young Persons Act 1933 (Section 53)***; or the ***Children and Young Persons (Scotland) Act 1937 (Section 57) (young offenders convicted of grave crimes)***.

88. Individuals rehabilitated under this Act are not, in general, required to disclose spent convictions and their careers cannot normally be prejudiced by a failure to disclose such convictions.

89. However, a knowledge of past convictions may be relevant to a security vetting enquiry in order to give an overall picture of the individual concerned to help assess the individual's trustworthiness. For this reason, the ***Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975***, permits spent convictions to be taken into consideration for the purposes of safeguarding national security.

90. In Northern Ireland, under the ***Rehabilitation of Offenders (Northern Ireland) Order 1978 (Exceptions) Order 1979***, in addition to the above, spent convictions may also be taken into account where the protection of public safety or public order is involved.

91. Individuals undergoing security vetting are required, in the Security Questionnaire, to provide details of spent convictions. The Act also permits spent convictions to be discussed with third parties, such as line managers and referees during the course of the security vetting process, without the adverse legal consequences which would otherwise follow such discussion. It also enables the refusal of security clearance on the basis of spent convictions even if such a refusal will have adverse consequences on the individual's career.

92. It is a criminal offence to reveal information about spent convictions except in the course of official duty.

Rehabilitation periods

93. Rehabilitation periods are calculated from the date of conviction as follows:

- For a sentence of imprisonment or detention in a young offender institution (previously youth custody) between 6 months and 2 years 6 months - 10 years.

- For a sentence of imprisonment or detention in a young offender institution of 6 months or less - 7 years.

- For a fine or other sentence, for example, a compensation or community service order received on or after 3 February 1995, for which the Act does not specify a different rehabilitation period - 5 years.

- For an absolute discharge - 6 months.

All the above periods, except for an absolute discharge, are halved if the individual convicted was under 18 years old. If an individual under 18 years old, received a probation order on or after 3 February 1995, the rehabilitation period is two years and 6 months or until the order expires, whichever is longer.

94. The following sentences could be imposed only on young individuals:

- Borstal - 7 years

- Detention centre - 3 years

- An order for custody in a remand home or an approved school order - A period ending 1 year after the order expires

95. The following sentences carry variable rehabilitation periods:

- A probation order, received before 3 February 1995, conditional discharge or bind over - 1 year, or until the order expires, whichever is longer

- A care order or supervision order - 1 year, or until the order expires, whichever is longer

- An attendance centre order a period ending - 1 year after the order expires

- A hospital order, with or without a restriction order - 5 years, or a period ending 2 years after the order expires, whichever is longer

96. In Scotland, supervision requirements made by children's hearings attract similar rehabilitation periods to care or supervision orders.

97. Details of all cautions recorded since November 1995 will be provided in response to a request to NIS for criminal record information. The provision of details of cautions before that date might not always be possible. It is, of course, open to Investigation Officers to make checks with local police in DV enquiries, but these should be limited to cases where there is a clear justification for doing so.

98. For specific guidance and recommendations concerning assessment, see ***Assessment of Vetting Information -*** refer to paragraph 165.

For CTC clearance

99. **[Redacted]**

For SC and DV clearance

100. To continue with the vetting or review process, proceed to the Credit Reference Check stage - refer to paragraph 101.

Stage 5 - Credit Reference Check

101. A Credit Reference Check should be made, on the subject only, with Experian Ltd using the 'Cabinetview' service. This service will provide departments and agencies ('Users') with access over the Internet to The Experian Credit Database. For online searches, each User will be issued with a digital certificate without which the service cannot be accessed. Thereby, transmission of data across telecommunications lines will be securely encrypted. A list of named authorised Users will also be held and there will be password protection. Similarly, for telephone/fax/post/e-mail enquiries, the individual Users' names will be checked together with passwords.

102. To make an enquiry, and to comply with 'Third Party Data' regulations, Experian require:

a. The individual's title (Mr, Mrs, Ms, Dr, etc) **(mandatory requirement).**

b. The individual's forename and surname **(mandatory requirement).**

c. The individual's date of birth **(mandatory requirement).**

d. The individual's full residential postal address (including house name and number, where both exist, and postcode) **(mandatory requirement).**

In respect to the mandatory points at a - d staff completing enquiries with Experian should note that if the individual's title and/or date of birth are unavailable, you may still proceed with the search. However, if for any reason there is more than one 'hit' (a 'hit' being a match on a person's details) when entering just the individual's name and address, there will be no return.

e. The individual's middle name(s), suffix and sex **(optional requirements).**

All the above details can be entered for current and up to two previous addresses. Any more than two previous addresses will require a separate enquiry.

For SC clearance

103. Departments and agencies may exercise discretion in respect of Credit Reference Checks for SC clearance as follows:

a. To restrict checks to addresses covering the last 3 years only, provided that no adverse financial information has come to light and that there is sufficient assurance about the individual to make a decision.

b. To exclude searches at addresses where the individual has lived for less than 9 months (excluding the current address).

c. To exclude searches at addresses which are clearly identifiable as student accommodation.

104. When a successful search has been completed, the screen will display a summary of the individual's financial status as well as access to the data received during the search. A search 'footprint' will be recorded which will only be available to the individual and other Users of 'Cabinetview' for a period of 12 months. Further information about the system is available from Experian.

Analysing the information received

105. The following information will be included in the detail provided by Experian:

Summary - refer to paragraph 106

Application details - refer to paragraph 108

Voters roll - refer to paragraph 109

Alias/associations - refer to paragraph 110

Public information - refer to paragraph 111

CAIS - refer to paragraph 112

CML - refer to paragraph 113

CAPS - refer to paragraph 114

Address links - refer to paragraph 115

GAIN - refer to paragraph 116

Director Report - refer to paragraph 117

Bronze Report - refer to paragraph 119

Print notes - refer to paragraph 120

Summary

106. This screen shows a summary of the information found under Voters Roll, Public Information, Previous Searches and CAIS. Warning Messages highlight information and provide links to report sections that may be relevant to the enquiry e.g. notice of correction, arrangement, reported gone away and previous address. Under the ***Consumer Credit Act 1974***, an individual can apply to have a 'Notice of Correction' placed on record indicating that, in their view, adverse information held by a credit reference agency is incorrect. The credit reference agency may not delete or vary such a notice.

107. The **Delphi Information** (credit opinion) is a generic risk assessment of the credit worthiness of individuals based on Experian's Credit Database information. It is an indication of the likely payment performance of the individual (given as a percentage), based on their existing credit records, public information and address data. The **Address Confirmation** indicates the data sources that were used to confirm the individual's address. The **Public Information** specifies the number of public information records that are present on the individual's file and the date of the latest case. The **Previous Searches** specifies the number of credit searches performed on the individual in the last 12months. The **CAIS** indicates the number of accounts held by the individual. The total balance of the active accounts is shown.

Application Details

108. This screen shows the mandatory and optional details that have been provided by the User.

Voters Roll

109. The Voters Roll holds the details of everyone who is registered to vote at almost every address in the UK and the Isle of Man. This information is updated each year to produce a complete record of everybody over the age of 18, or who will soon be 18. As the Voters Roll is classed as public information, this section will display information on all people registered at the address provided by the User. Where the information does not reflect that given on the Security Questionnaire, the individual should be asked to clarify the information. In most cases, a genuine mistake is more likely than a deliberate attempt to mislead. **[Redacted]**

Alias/Associations

110. This section displays details of all known aliases and financial associations of the individual that have been entered for the current enquiry or returned from the credit search.

Public Information

111. This section displays public information records for the individual covering the last 6 years e.g. county court judgments (CCJs), Scottish decrees, bankruptcies, voluntary arrangements, bills of sale, certificates of satisfaction and administration orders and is compiled by Experian using information from the Registry Trust Limited, official gazettes and the insolvency service. Where an individual has been served CCJs or Legal Notices it may be necessary to ask the individual to complete a Financial Questionnaire, but where these are more than 6 years old, this may not be considered necessary. In the case of bankruptcy, the individual should always be asked to complete a Financial Questionnaire.

Credit Account Information Sharing (CAIS)

112. CAIS is the largest source of consumer credit histories in the UK. It holds information on over 260 million credit accounts, averaging 3 records per application (although any one individual can have an unlimited amount of CAIS accounts), covering over 80% of the active credit population. A number of credit accounts are shared between Experian and their major competitor, which accounts for Experian having 70% market share. Due to the amount of data that may be available, a summary of the CAIS records are provided - displaying account performance for the last 3 years - and a link provided to a detailed account of each case. It is difficult to give a figure for the number of credit commitments above which there should be cause for security concern. The analysis of this information is largely dependent on the age and general financial circumstances of the individual. Where the rest of the report does not give cause for security concern, even a large number of credit commitments is unlikely to justify further investigation. It is for DSOs, taking into account their local circumstances, to decide the threshold beyond which cases should be referred to the assessor.

Council of Mortgage Lenders (CML)

113. This section shows all the records supplied to Experian by the CML, from its Repossessions Register, covering the past 6 years. It is used to check whether the individual has previously had their home repossessed or given it up voluntarily.

Credit Application Previous Searches (CAPS)

114. CAPS is the UK's largest file of credit reference enquiries relating to credit applications made by individuals. This section shows all the CAPS records registered for the individual as a result of a credit application over the last 12 months, by quarters. A total of five applications would not be unusual; and more than five should not be of immediate concern unless there are other indications that the individual has financial problems and could be applying for excess credit. More than ten applications would indicate the need to consider asking the individual to complete a Financial Questionnaire. Credit applications do not necessarily result in the taking up of credit, but may indicate underlying reasons for the individual considering such activity.

Address links

115. This section lists all of the addresses associated with the individual using information from Experian's Credit Database. The existence of information about the individual at either a previous or forward address does not necessarily indicate that it is adverse. Where there are no other indications in the report that would give cause for security concern, further investigation of a forward or previous trace is unlikely to be necessary. Where there are other indications, the individual should be asked about the addresses outside the period requested on the Security Questionnaire.

Gone Away Information (GAIN)

116. GAIN is an information exchange network that stores up-to-the-minute information about customers who are in arrears on credit contracts and have moved without leaving a forward address. This section displays details from a credit company showing that they have been informed that an individual has moved from the address, but then another company has had a subsequent dealing with that person at the same address.

Director Report

117. When a User performs a search, the Cabinetview Report can show whether the individual searched is a director. If details are returned, the name and address of the director will be shown in the Director section. A Director and Secretary Report can then be requested by clicking on the name of a director. A Director and Secretary Report provides information on the individual including current, previous, dissolved directorships, Secretaryships and partnerships in addition to any convictions and disqualifications. It will also list full details of any Notices of Corrections related to this director. If information about convictions or disqualifications has been found, a warning message will be displayed at the top of the report. Names and registered numbers of the company(ies) will be provided. Dates of appointments, resignations and dissolutions, where appropriate will be provided. The latest event changing the status of the company will also be shown.

Republic of Ireland

118. Experian now also offers an off-line service provided by its Consumer Help Service, enabling users to process vetting applications for those that contain addresses within the Republic of Ireland. The cost of this service will be £5.00 per Consumer Details application and £7.95 per Company Details application. A form is provided by Experian to be completed by the users, detailing the user's name, full address, phone number, fax number, signature, Experian account number and Experian Branch number, applicant's full name, date of birth (if known) and addresses to be searched. This form can then be faxed to Experian's Consumer Help Service, who will carry out the search on the user's behalf and fax the results back to the user.

Bronze Report

119. From the Director and Secretary Report, the User can order a Bronze Report (at additional cost) containing information about the company(s) associated with the director. This report will include the corporate structure, summary accounts, credit rating, credit opinion and risk score, and the names of Directors and Secretaries. Experian's risk scores and credit ratings are probability opinions provided for guidance. Experian offers no guarantee that companies awarded a particular score will perform in a certain way.

Print Notes

120. Users can use this section to record their own comments. These will be included on the printed report but will not be saved.

121. **[Redacted]**

[Redacted]

122. **[Redacted]**

[Redacted]

123 **[Redacted]**:

[Redacted]

[Redacted]

[Redacted]

124. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

125. **[Redacted]**:

[Redacted]

126. **[Redacted]**

127. **[Redacted]**

[Redacted]

[Redacted]

128. **[Redacted]**

129. **[Redacted]**

130. **[Redacted]**

131. **[Redacted]**

132. **[Redacted]**

[Redacted]

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

[Redacted]

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

[Redacted]

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

133. **[Redacted]**

134. **[Redacted]**

135. **[Redacted]**

136. **[Redacted]**

[Redacted]

137. **[Redacted]**

138. **[Redacted]**

[Redacted]

139. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**.

    c. **[Redacted]**.

140. **[Redacted]**

[Redacted]

141. **[Redacted]**

Stage 7 - Review of personal finances

142. The individual should be asked to complete a Financial Questionnaire (FQ). A new, scannable FQ will be introduced alongside the redesigned DV questionnaire. Existing forms should be used until the new FQ is made available.

143. The aim of a financial review is to highlight current or potential concerns which may require further investigation or provide the basis for discussion during the Subject Interview stage of the security clearance process.

144. The information recorded on the Financial Questionnaire seeks to address 6 areas of concern:

a. Previous financial unreliability, for example, bankruptcy.

b. Problems meeting current financial commitments.

c. Poor financial judgement.

d. Possible future financial difficulties.

e. Assets and habits inconsistent with income.

f. Other conflicts of interest.

An assessment of this information given by the individual on the Financial Questionnaire, should be made against the scoring system and criteria set out in the ***Assessment of Vetting Information -*** refer to paragraph 165.

145. **[Redacted]**

146. To continue with the vetting or review process, proceed with the Subject Interview and Further Enquiry stage.

Stage 8 - Subject interview and further enquiries

147. The subject interview is the most important element of the DV process **[Redacted]**

For CTC and SC Clearance

148. The subject interview should not normally form a part of either the CTC or SC security vetting process, but may be considered if there are unresolved security concerns about the subject, **[Redacted]** The vetting authority must be able to demonstrate that there is clear need for such an interview.

149. **[Redacted]**

[Redacted]

150. **[Redacted]**

151. Where there are no adverse indicators from the initial vetting clearance, and the subject has a complete annual SAF record with no adverse indicators, no subject interview need be carried out at second and subsequent review.

Further Enquiries

152. Further enquiries take the form of interviews with referees, either nominated by the individual or 'developed' by the Field Investigating Officer (FIO). The purpose of the interviews is to provide an independent, reliable view of the subject, of sufficient depth, and covering a period of at least the past 10 years of the subject's life.

153. **[Redacted]**

154. **[Redacted]**

155. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**.

156. The inquiries should also include:

    a. The individual's line manager, or a supervisor at school, college or university (where appropriate).

    b. A previous line manager if the current line manager has known the subject for less than one year.

157. If any unresolved issues of security significance remain outstanding, or where the required level of assurance has not been reached, further enquiries may be

undertaken. It is important that the vetting authority is able to demonstrate the need for further enquiries.

Record of Factual Content of Interview

158. Any factual information in the investigator's report should be seen and agreed by the subject prior to the report being submitted where practicable. It is particularly important for the subject to agree to the content of the investigator's report in cases where the likely outcome is refusal or withdrawal of clearance, and hence where there is a possibility of an appeal internally, to the Security Vetting Appeals Panel, or an Employment Tribunal.

159. No decision to grant, refuse or manage a DV (or CTC/SC where the interview was invoked) clearance should be taken until each element of the information gathered during the process has been considered and documented.

160. There will be other cases where the degree of assurance as to the individual's reliability will require more intensive enquiries to give a satisfactory degree of assurance. These include:

    a. **[Redacted]**

    b. Where a young person may not have reached full maturity.

    c. Where information of security significance has been highlighted during the course of the DV process – decisions on how to make enquiries in this case will need to be considered very carefully, on a case by case basis.

161. Withholding information from the Investigating Officer may deny a possible lead to a line of enquiry. This could result in a devaluation of the Subject Interview and subsequent enquiries which may adversely affect the Investigating Officer's final report.

162. The Investigating Officer may request local Police HQ (excluding MPSB) to make checks against their own records or other appropriate enquiries about the individual

(but no one else) where there is a clear reason for doing so. Where appropriate, the Investigating Officer may initiate a check with the Police Adult Caution Index and/or the Juvenile Index.

163. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

164. **[Redacted]**

Assessment of Vetting Information:

Adjudicative Guidelines for Clearance Decisions

Introduction

165. The adjudicative guidelines (Appendix 7) are designed to provide assistance to assessors in determining the level of risk posed by any adverse indicators associated with the subject. They should be read in conjunction with this section. Although they are intended principally for DV, they may also be used to assist with the assessment of CTC and SC clearances, since most of the same aspects of the subject are investigated.

166. **[Redacted]**

167. **[Redacted]**

168. **[Redacted]**

Other Considerations

169. There are disadvantages to carrying out security vetting on recent recruits to government service since departments and agencies will, in general, have less knowledge about the individual's character, interests and opinions. The more direct knowledge about the candidate's character, interests and opinions, the greater the

value of the vetting process. Individuals who are new or recent recruits should not normally be considered for posts which require DV clearance.

Adverse indicators in current records

170. Departments and agencies should consider carefully whether or not to proceed with the security vetting process where:

    a. The individual has previously been refused a security clearance or had a clearance withdrawn.

    b. There is any adverse information about the individual's character, behaviour or circumstances which is likely to lead to refusal.

171. Before deciding not to proceed, further consideration should be given where:

    a. A sufficient period of time has elapsed since the adverse information was recorded without any further problems.

    b. Government policy has changed in respect to the denying or withdrawal of a security clearance.

    c. A previous decision was borderline or the individual's circumstances have changed sufficiently to justify reconsideration.

172. In all these instances an initial interview with the individual should be considered to clarify the latest position.

173. Providing there are no overriding adverse indicators against proceeding with the process of clearance, assessors should take account of the guidance that follows.

Making security clearance decisions

Responsibility for Clearance Decisions

174. When the subject is already employed, the vetting unit will make a recommendation as to whether or not the subject is suitable to hold a clearance, based on the nature and severity of any adverse information, balanced by positive information and mitigating circumstances. However, the ultimate responsibility for an employment decision rests with the employer or contracting authority. Where a subject presents a security risk, the employer or contracting authority must decide whether or not the risk is manageable. The vetting unit will give advice on how the risk can be managed. The vetting unit and/or employer's security unit will design a programme to ensure that this is maintained (including contractors). When the subject is not currently employed, delegated authority arrangements for clearance decisions between the employer or contracting authority and the vetting unit will apply.

175. Where the assets at risk are not those of the Department alone **[Redacted]** the Department must additionally involve the asset risk owner as follows:

    a. Where the vetting unit judges that an issue is not significant, the risk owner need only be informed;

    b. Where an issue is significant but the employer or contracting authority believes that the risk can be managed, they should consult the risk owner before reaching a decision;

    c. Where the employer or contracting authority are not satisfied that the risk can be entirely managed but believe that it is in the wider national interest for any residual risk to be accepted, they must seek the prior approval of the risk owner whose decision will be final.

Risk Factors and Considerations

Adjudicative Guidelines

176. As already mentioned, detailed guidance on the interpretation of information gathered during the vetting process is given in the Adjudicative Guidelines (Appendix 7).

General Considerations

177. The vetting officer must use the available evidence to judge whether or not adverse information reflects a recent or recurring pattern of questionable judgement, irresponsibility or emotionally unstable behaviour.

178. When considering the security impact of personal circumstances or behaviour that can lead to vulnerability, the assessor must not allow personal and cultural bias to affect their judgement. Personal circumstances or behaviour only become of security significance if they cause vulnerability to pressure or improper influence or are likely to result in the subject committing security breaches.

    a. The nature, likelihood and credibility of the threat;

    b. The nature, value, vulnerability and sensitivity of assets under threat;

    c. The damage resulting from the compromise of these assets;

    d. The relevance of security information concerning the subject in the light of a, b and c above.

179. Any assessment of the level of security risk entailed by the subject's conduct should be based on:

    a. The nature, extent and seriousness of the conduct;

    b. The circumstances under which it took place e.g. knowing participation;

    c. The frequency of the conduct and when it took place;

    d. The subject's age and maturity at the time;

    e. Whether or not the subject's participation was voluntary;

    f. The presence or absence of rehabilitation and other behavioural changes;

    g. The motivation for the conduct;

    h. The potential for associated pressure, coercion, exploitation or duress;

i. The likelihood of continuation or recurrence.

CTC and SC Clearances

180. Clearance decisions should only be made once all available information has been received, recorded and assessed. The following factors should be taken into consideration:

a. Known associations with organisations or representatives of foreign powers hostile to the UK or to the pursuit of Parliamentary democracy.

b. The existence of fundamental conflicts of interest because of membership or association with, for example, certain pressure groups or connections to foreign interests either directly or through family, partner, friends or business interests.

c. The demonstration of a lack of integrity by deliberately withholding or falsifying information relevant to the security vetting process.

d. The demonstration of unreliability by infringing security regulations or by being indiscreet about confidential matters.

e. The demonstration of dishonesty or lack of integrity, for example, by being convicted of a serious criminal offence, or a series of offences, which indicate habitual criminal tendencies or serious behavioural vulnerabilities.

f. Vulnerability to financial inducements including serious, unresolved financial difficulties.

g. Illness or mental condition which may seriously impair judgement or unintentionally create a risk to security.

h. Vulnerability to indiscretion, inducement or improper influence because of addiction to or indiscriminate use of alcohol or drugs (including misuse of legal/prescription drugs and medicines).

i. Susceptibility to pressure or improper influence, for example, because of current or past conduct.

181 While adverse information in any one of these categories might provide grounds to refuse clearance, a risk management approach should be taken to assessment. Clearance should be denied only where adverse information presents a risk that cannot be managed in the context of extant threats and vulnerabilities, and the likely consequences of a breach.

DV Clearances

182. Assessment at the DV level needs to take full advantage of the greater breadth and depth of evidence available **[Redacted]** As with CTC and SC, clearance decisions should only be made once all available information has been received, recorded and assessed.

183. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

j. **[Redacted]**

k. **[Redacted]**

l. **[Redacted]**

m. **[Redacted]**

n. **[Redacted]**

184. **[Redacted]**

185. Except on recruitment, individuals must always be informed of the outcome of their security vetting case as it may affect their future postings and career prospects. Where a security clearance is refused, withdrawn or limited, departments and agencies should consider if a security clearance at a lower level would be justified, where the criteria for security clearance may need to be less stringent. In its judgment on the Leander case (1987), the European Court of Human Rights acknowledged that a wide margin of appreciation must be afforded to a state in assessing the requirements of national security and in designing appropriate systems for its protection. In order to continue to enjoy that margin of appreciation it is important that individual security vetting decisions are made on the basis of standard criteria applied to all of the facts of each case. To achieve this objective, every effort must be made to establish the facts and resolve any apparent discrepancies which are revealed or doubts to which they give rise.

186. At all times departments and agencies must:

    a. consider each case solely on its merits;

    b. record clearly the reasons for the decision arrived at;

    c. be prepared to defend that decision if challenged.

[Redacted]

Action on completion of security vetting

187. The vetting unit/employer can take the following actions:

    a. Grant (or renew) clearance – where there is no adverse information of security significance concerning the subject, clearance should be granted without limitations. The subject's clearance will be managed actively as detailed in 'maintenance of effective personnel security' below.

b. Refuse (or withdraw) clearance – where adverse information has sufficiently serious security implications that the employer is not able to properly manage the risks arising from it.

c. Grant clearance with limitations – where adverse information has security significance but the risks presented are manageable. The programme of ongoing management should reflect and address the risks identified.

Notification of security clearance decisions

188. For the vetting system to have the confidence of employees and be defensible publicly, it is important that individuals are given as much information as possible about their security clearance and made aware that there is an effective appeals mechanism.

Approving security clearance

189. Where a security clearance is approved, any reservations should be clearly recorded. DV security clearances should be recorded by means of a formal certificate.

190. The individual should be informed by the DSO or List X Contractor, as appropriate, that security clearance has been approved. This is not necessary for a review of the individual's security clearance, but it may be decided that it is preferable for management to do so. Notification gives a useful opportunity to remind individuals of their responsibilities for protecting the assets they work with and that personnel security is an on-going process. Individuals should be encouraged to feel that they can freely report any security concerns to line managers, the security branch or to personnel management, with confidence that their concerns will be dealt with sensitively and sympathetically.

Transfers loans and moves

191. The move, transfer or loan of any individual to a post requiring a security clearance should not take place until the receiving organisation has received confirmation of appropriate security clearance.

192. An individual holding a current security clearance can carry it if they move, transfer or are loaned to another government department, agency or List X contractor. The receiving organisation is responsible for ensuring that an individual has the correct level of security clearance.

193. The following conditions must be applied when transferring a security clearance to another organisation:

    a. Initial and revalidated security clearances must not be more than 10 years old;

    b. There must not have been more than 1 year between leaving one organisation and joining another;

    c. The individual must not have resided overseas for more than 6 months during that break in service.

Acceptance or rejection of a transfer or loan

194. Where an individual with a security clearance is being transferred or loaned, there is no obligation on the receiving organisation to proceed with the transfer if, after examination of the relevant information, they assess the individual is not suited to fill the post on security grounds. If possible, the individual should not be notified of the proposed move until all security considerations have been met. In some cases, the receiving organisation may only be able to give provisional agreement to a move, pending appropriate security clearance.

Transfer of security records

195. Once an appointment has been agreed and if the individual is moving to a post that requires a security clearance, the security records should be handed over to the receiving department, agency or List X contractor, which will then be responsible for aftercare procedures and security clearance reviews. For loaned staff, these papers will be held by the receiving organisation which will be responsible for carrying out security clearance reviews as required during the period of loan. Where the individual

does not have an SC clearance, the receiving organisation is responsible for initiating the SC vetting process - refer to paragraph 33.

196. When the individual does not require a security clearance in the new post, particularly where their security clearance has been refused or withdrawn in the past, the supplying and receiving organisations should agree an appropriate treatment of the individual's security records. If the records contain particularly sensitive material, it may be appropriate for the supplying organisation to retain them. In such cases, there should be a clear note on the individual's personnel file instructing the receiving organisation to consult the supplying organisation before the individual is considered for any security clearance.

[Redacted]

197. **[Redacted]**

For CTC and SC clearance

198. Where an individual moves to a post requiring a CTC or SC clearance, it is sufficient for the receiving organisation to receive a written or oral assurance that a CTC or SC clearance is held by the individual and that no information of security concern exists on record. However, where there is such information on the individual's record the receiving organisation, or Contracting Authority for List X firms, must examine the relevant papers before the individual moves. Where the individual does not have a CTC or SC clearance, unless otherwise agreed, the receiving organisation (or Contracting Authority for List X firms) is responsible for initiating the CTC - refer to paragraph 28 - or SC - refer to paragraph 33 - vetting processes.

For DV clearance

199. Where an individual moves to a post requiring a DV clearance, the receiving organisation (or Contracting Authority for List X firms) must examine all relevant records before the individual moves. Where the individual does not hold a DV clearance, unless otherwise agreed, the receiving organisation (or Contracting

Authority for List X firms) is responsible for initiating the DV vetting process - refer to paragraph 38.

Movement of individuals from List X contractors

For CTC and SC clearance

200. Where an individual moves to a post requiring a CTC or SC clearance, and the individual has been allocated a 500 or AA security clearance reference, it is sufficient for the receiving organisation to receive a written or oral assurance that a CTC or SC clearance is held by the individual and that no information of security concern exists on record. Where there is such information on the individual's record, or where a 500 or AA reference is not given, the receiving organisation (or Contracting Authority for List X firms) must examine the relevant papers before the individual moves. Where the individual does not have a CTC or SC clearance, unless otherwise agreed, the receiving organisation (or Contracting Authority for List X firms) is responsible for initiating the CTC - refer to paragraph 28 - or SC - refer to paragraph 33 - vetting processes.

For DV clearance

201. Where an individual moves to a post requiring a DV clearance, the receiving organisation (or Contracting Authority for List X firms) must examine all relevant records before the individual moves. Where the individual does not hold a DV clearance, unless otherwise agreed, the receiving organisation (or Contracting Authority for List X firms) is responsible for initiating the DV vetting process - refer to paragraph 38.

[Redacted]

202. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

Adverse vetting decisions

Refusing security clearance - existing employees

203. Where security clearance is refused for an existing employee, the reasons for the decision should be recorded in full on the individual's record. The individual should be informed promptly in writing that their security clearance has been refused and, so far as is possible, given the reasons for the refusal related to the relevant facts. In some cases, considerations of security or confidentiality may prevent this. The proposed appointment of the individual should not be made and they should be informed, fully and clearly, of the mechanisms for internal and external appeal.

204. Where a refusal of security clearance is as a result of information obtained from a Criminal Record Check or financial enquiries, the individual should already have been shown the original information used to support the decision. Where an interview took place, the individual should have agreed a factual account of any concerns.

205. **[Redacted]** Should the individual wish to take this further, the normal grievance procedures, with the right of appeal to the Head of Department and, ultimately, the Security Vetting Appeals Panel, should be followed. **[Redacted]**

206. Unless the reasons for refusal are connected with a serious disciplinary matter, an individual who is refused a CTC, SC or DV clearance should continue to be employed. In a department or agency where the proportion of highly protected assets is small, this should present little difficulty. Where security objections are such that the department or agency can not continue to employ the individual, and no other post can be found, it may be necessary to consider if dismissal on security vetting grounds is warranted.

Refusing security clearance - on recruitment

207. There is no requirement to inform an individual of the reasons why they have been refused employment. Where the decision to refuse is solely on security grounds, the individual should preferably be told of the reasons, as this may have an impact on any

future employment applications. In some cases, considerations of security or confidentiality may prevent explanation.

208. Where it is clear to the individual that the decision to refuse employment was directly related to the need for security clearance, the individual may wish to challenge the decision, although the remit of the Security Vetting Appeals Panel does not extend to applicants for employment. **[Redacted]**

Withdrawing security clearance

209. Where a decision is made to withdraw a CTC, SC or DV clearance, the procedure is the same as that for refusal of a security clearance. The possibility of approving a security clearance at a lower level should be considered.

Limiting security clearance

210. Where there are limitations on an individual's security clearance, the individual should normally be told of the limitations and, so far as is possible, given an explanation. There may be exceptional circumstances where it will not be possible to do so, for example, in cases of mental illness or incapacity **[Redacted]** The individual should then have the option, where appropriate, of seeing the factual information that was used to support the decision in the same way as if they had been refused a security clearance. **[Redacted]**

Informing individuals of the reasons for an adverse vetting decision

211. Where the individual is given the reason for refusal, withdrawal or limitation of a security clearance, departments and agencies may explain the particular criteria used. Where possible the individual should be given the evidence that supports the decision, for example, Criminal Record Check, results of financial enquiries, past infringement of security regulations. In some cases, the individual will need to be handled particularly sensitively as it may be difficult to disclose the reasons for refusing security clearance, for example, an individual's mental instability.

212. There will also be cases where essential supporting evidence can not be disclosed to the individual, **[Redacted]**. In other cases, essential evidence may have been obtained from confidential interviews made in the course of the security vetting process. Such information may only be disclosed if:

a. It was given by the individual's senior managers or colleagues;

b. It relates directly to the individual's performance of their duties;

c. The individual who has given the information agrees that it may be disclosed.

213. Legal advice should be sought before any other information, derived from confidential enquiries, is disclosed to the individual. This is to protect the originator of the information against possible libel or slander action.

Challenging an adverse vetting decision

214. All departments and agencies must have in place an internal appeals process to consider challenges by individuals to adverse security clearance decisions **[Redacted]** Where an individual has exhausted the internal appeals process but remains dissatisfied with the outcome, the individual may seek to appeal to the Security Vetting Appeals Panel or may use other legal processes - refer to paragraph 268.

215. It is an accepted principle of the vetting system that any information obtained during the vetting process, particularly from third parties, will be kept in confidence. In certain cases it is possible that details might come to light which suggest criminal or other activity where there is an overriding responsibility to inform the relevant authorities. There may be circumstances where it is appropriate to share some information with personnel or line management in order that a risk may be adequately managed. Such cases should be rare and handled with great care. The permission of the originator should be obtained before disclosing any details given in confidence. The general principle of confidentiality should be maintained in all but the most exceptional cases.

Review of security clearances

General Points

216. When used properly and appropriately, baseline recruitment checks and vetting are highly effective initial screening tools. However, the checks and interviews carried out during the initial recruitment and vetting processes provide only a snapshot of an individual at a given point in time. It is also noteworthy that the majority of spies, leakers and others who in some way have betrayed their organisations (a) passed through these screening processes without adverse indicators and (b) had no intention of betrayal at the time they joined. Most employees become disloyal due to some change in their circumstances so the main threat to organisations comes from those already inside. One notable exception to this is investigative journalists attempting to penetrate an organisation in search of a story.

217. While the vetting system is geared in part towards identifying those with the potential for future disloyalty, this is in practice extremely difficult. On top of this, the vast majority of government employees and contractors are not vetted in any case. Therefore pre-employment checks and vetting must be regarded as just the beginning of an ongoing and actively managed personnel security regime aimed at managing those residual risks to organisations that cannot be addressed by pre-employment checks and vetting.

Role of Line Managers and Supporting Organisations

218. Line management has a fundamental role to play in the maintenance of personnel security (see Appendix 8: Line Manager's Guide). This applies equally whether the manager and/or staff hold clearances or not. **[Redacted]**:

    a. **[Redacted]**

    b. **Redacted]**

    c. **Redacted]**

    d. **Redacted]**

    e. **Redacted]**

f. **Redacted]**

g. **Redacted]**

219. **Redacted]**:

a. **Redacted]**

b. **Redacted]**

c. **Redacted]**

220. **Redacted]**

221. **Redacted]**

Security Awareness and Education

222. It is important that departments foster a culture of security awareness and education. The majority of public sector and associated contractor staff do not hold a national security clearance and therefore will not have their background checked beyond what is laid down in the Baseline Personnel Security Standard. While these staff will not by definition be employed in posts with major national security sensitivities or under direct threat from terrorism, it is important that they understand their responsibility to protect the assets that they own and use and that Line Managers understand their responsibility to ensure that appropriate, ongoing personnel security measures are maintained. It is equally important that line managers have ready access to support from HR, occupational health and welfare services and security to enable them to manage sometimes complex and cross-cutting problems.

Review of Baseline Checks

223. There is no formal requirement to renew or review a baseline check where the subject has been continually employed by the same department, agency or List X contractor throughout the review period. However, there are some circumstances where a review is appropriate (please refer to the Baseline Personnel Security Standard (see MR 23)).

Formal Processes for Ongoing Management of National Security Clearances

224. Where a staff member holds a national security clearance, there are two formal processes in place that may be used to assist in the ongoing management of those clearances, namely, periodic review of clearances and the annual Security Appraisal Form (SAF).

Review of Personnel Security Clearances

225. Security clearances should be subject to periodic review:

a. In the light of any adverse information received subsequently to vetting.

b. To follow up adverse indicators identified in the original vetting process.

c. At regular intervals as shown below. Note that these review periods are a minimum standard and that clearances may be reviewed more regularly at the discretion of the employer.

[Redacted]:

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

[Redacted]:

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

226. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

Standard for Reviews

CTC and SC

227. The review periods outlined above should be rigorously applied, and should be shortened at the discretion of the vetting authority where early review would assist the management of security risks associated with the subject.

228. The sequence of checks made for the initial clearance should be repeated (except for baseline checks) to ensure that all information held on the subject is up to date and that any changes that may have security significance can be followed up. If any additional checks were carried out, such as a subject interview, these may also be repeated at the discretion of the vetting authority.

229 Employers must ensure that any information with security implications identified in a review is properly recorded, followed up and assessed. Where any changes to a subject's clearance status are made as a result of information arising at review, it is important that a proper audit trail is available.

DV

230. As for CTC and SC, the recommended review periods for DV clearances represent a minimum standard and should be shortened where early review would assist in the management of security risks associated with the subject.

231. The sequence of checks made for the initial clearance should be repeated (except for baseline checks) to ensure that all information held on the subject is up to date and that any changes that may have security significance can be followed up. In addition:

a. All first DV reviews must include a face-to-face interview with the subject.

b. At first review, at least one face-to-face interview with a referee should be carried out. Preferably the referee will be the supervising officer that has known the subject best since the initial clearance was granted.

c. If there are no adverse indicators from the initial vet and the subject has a complete SAF record with no adverse indicators, then no subject interview needs to be carried out at the second and subsequent reviews.

232. Vetting authorities must ensure that any information with security implications identified in a review is properly recorded, followed up and assessed. Where any changes to a subject's clearance status are made as a result of information arising at review, it is important that a proper audit trail is available.

Annual Security Appraisal Form (SAF)

233. A SAF is required annually for all DV clearance holders and in some circumstances for CTC or SC holders. The SAF is split into two parts, one to be completed by the subject and one by his/her line manager, which should be returned to the unit which carried out the initial clearance. A sample SAF is Attached at Appendix 3. Provided that the same information is provided, departments may customise the form and the process described below to suit local needs.

234. **[Redacted]**

235. The purpose of the SAF is to identify any changes in the subject's circumstances, personality and/or behaviour since vetting was carried out, and the form and process used should meet the following requirements:

a. The process must be based on an up-to-date appreciation of security concerns in order to adequately guideline managers in highlighting any potential vulnerability of cleared staff. Appropriate guidance must be provided by employers to line managers and staff.

b. The SAF must reflect those areas about which it is reasonable to expect line managers to provide information.

c. Lines of responsibility and accountability for acting on adverse information must be clearly defined.

d. All employing departments or agencies must institute effective auditing of the SAF process alongside the other stages of vetting.

e. The SAF should consist of two parts. The whole SAF should be sent to the subject. The subject should complete part 1, declaring any changes in personal circumstances and then pass the SAF to his/her supervisor to complete part 2.

f. The supervisor who has known the subject best during the SAF period should complete part 2.

g. Both parts of the form should be returned to the vetting unit at the same time. Should the subject not wish his/her line manager to see any information that they have disclosed in the SAF, they should have the option of removing part 1 and providing this to the line manager inside a separately sealed envelope.

h. If either the subject or the line manager needs to disclose sensitive information on the SAF, then the final protective marking of the completed SAF may need to be reconsidered.

Change of personal circumstances

236. Individuals with CTC, SC and DV clearances should be made aware of their responsibilities for reporting any significant change to their personal circumstances. In particular, additional checks are required if there is a new partner. Whilst a change in the individual's partner's circumstances may involve marriage, or remarriage, there is no need to carry out a further check if the partner's details were included on the individual's last Security Questionnaire.

237. Where personal circumstances alter significantly, for example, change of partner, step-parent, step brother or sister, the individual should be asked to complete the relevant sections of the Change of Personal Circumstances questionnaire.

238. On return of the questionnaire, the following actions should be taken:

    a. Check the questionnaire has been correctly completed.

    b. Check the CTC, SC or DV box at the top of Page 1 has been ticked, as applicable.

    c. Check the individual has signed and dated the declaration on Page 5.

    d. Complete the sponsor's declaration on Page 5.

For List X contractors - For CTC and SC clearance

239. The individual should be asked to report a change of partner using a Security Questionnaire. It should be made clear why the questionnaire needs to be completed, by asking the individual to read the government's vetting policy on Page 2. The questionnaire must be marked, in red ink, at the top of Page 1, 'Change of Personal Circumstances'.

240. The individual should be asked to complete the following:

    a. Page 1 - in full;

    b. Page 3 - details about the individual - questions 1-4;

    c. Page 3 - details about the individual's partner - questions 8-14;

    d. Page 9 - the declaration at the bottom of the page.

241. On return of the questionnaire, the following actions should be taken:

    a. Check the questionnaire has been correctly completed.

    b. Check the CTC or SC box at the top of Page 1 has been ticked, as applicable.

    c. Check the individual has signed and dated the declaration on Page 9.

    d. Complete the sponsor's declaration on Page 12.

For List X contracts where the Contracting Authority is MOD or where MOD is involved: MOD DVA

242. Providing there is no adverse information as a result of checks and enquiries, the MOD will advise the Security Controller accordingly. Where there is an adverse result of enquiry or check the MOD will advise the Security Controller. Where there is difficulty in resolving a vetting case, DVA(MOD) will advise the Security Controller of the delay.

243. **[Redacted]**

For List X contracts where the Contracting Authority is not MOD and where MOD work is not involved: The Contracting Authority

244. Providing there is no adverse information as a result of checks and enquiries, the Contracting Authority will advise the Security Controller accordingly. Where there is an adverse result to enquiries and checks, or where there is difficulty in resolving a vetting case, the Contracting Authority will advise the Security Controller. Where there is difficulty in resolving a vetting case, the Contracting Authority will advise the Security Controller of the delay.

For Non-List X contracts: The Contracting Authority

245. The Contracting Authority will assume responsibility for the remainder of the security clearance process and will advise the contractor of its decision.

For DV clearance

246. The Security Controller should contact the Contracting Authority to request a Change of Personal Circumstances Questionnaire.

247. It should be made clear why the questionnaire needs to be completed, by referring the individual to the government's vetting policy on Page 2. The individual should complete the questionnaire as appropriate.

248. On its return the following actions should be taken:

a. Check the questionnaire has been correctly completed.

b. Check the DV box at the top of Page 1 has been ticked.

c. Check the individual has signed and dated the declaration on Page 5.

d. Complete the sponsor's declaration and certificate on Page 5.

The Security Controller should include the name and address of their site at the bottom of Page 5, even though it is not specifically requested by the questionnaire.

249. Send the completed questionnaire to the Contracting Authority who will assume responsibility for the remainder of the process and advise the Security Controller of its decision. If the declaration and certificate is not signed and dated, the questionnaire will be returned to the sponsor for completion.

Information received from the police

250. Chief Officers of police report convictions (except for minor motoring offences), cautions, reprimands and final warnings of civil servants to the Cabinet Office, who pass on the information to the individual's department or agency. There is a standing obligation for civil servants under the ***Civil Service Management Code*** to inform their employer if they are arrested and refused bail, or if they are found guilty of any criminal offence (except traffic offences unless an official car was involved, or the penalty involved imprisonment or disqualification from driving).

251. Where an individual holds a security clearance, the DSO should inform them that such a report has been received from the police. The DSO may also discuss the report openly with the individual.

252 There is no automatic reporting of criminal convictions of individuals employed by List X contractors.

[Redacted]

253. **[Redacted]**

254. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**

    d. **[Redacted]**

255. **[Redacted]**

Aftercare

Audit and Assurance for National Security Vetting

[Redacted]

256. **[Redacted]**

257. **[Redacted]**

258. **[Redacted]**

[Redacted]

259. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

260. **[Redacted]**:

    a. **[Redacted]**

b. **[Redacted]**

261. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

262. **[Redacted]**

[Redacted]

263. **[Redacted]**

[Redacted]

264. **[Redacted]**

265. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

266. **[Redacted]**

267. **[Redacted]**

Challenging vetting decisions

268. Depending on the circumstances of the case, an individual who wishes to challenge an adverse vetting decision may invoke one or more of the following avenues:

    a. An internal appeal – **[Redacted]**– followed, if necessary and assuming it falls within its remit, by an appeal to the independent Security Vetting Appeals Panel - **[Redacted]**

    b. Proceedings before an Employment Tribunal – under the:

        - **Employment Rights Act 1996 -** see paragraph 292
        - **Race Relations Act 1976 -** see paragraph 294
        - **Sex Discrimination Act 1975 -** see paragraph 299
        - **Disability Discrimination Act 1995 -** see paragraph 303

    c. Proceedings under the Fair Employment and Treatment (Northern Ireland) Order 1998 - see paragraph 304.

    d. An application under the Data Protection Act 1998 - see paragraph 309.

    e. An application for Judicial Review - see paragraph 313.

    f. Proceedings under the Human Rights Act 1998 - see paragraph 314.

    g. A complaint to the **Investigatory Powers Tribunal** - refer to paragraph 316.

269. Departments and agencies should be aware that challenges under any of the Acts or processes may involve potential risks to national security. In order to deal with these risks, some of the statutes contain provisions allowing a certificate of exemption to be obtained from the Minister on national security grounds. A department which is concerned with any such challenge which is likely to have implications for national security, must consult the Cabinet Office promptly, as well as informing their central management - including the Principal Establishment Officer and the Departmental Security Officer.

[Redacted]

270. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

[Redacted]

271. **[Redacted]**

[Redacted]

272. **[Redacted]**:

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

273. **[Redacted]**:

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

274. **[Redacted]**

[Redacted]

275. **[Redacted]**

276. **[Redacted]**

[Redacted]

277. **[Redacted]**

278. **[Redacted]**

279. **[Redacted]**

280. **[Redacted]**

281. **[Redacted]**

282. **[Redacted]**

283. **[Redacted]**

[Redacted]

284. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

285. **[Redacted]**

286. **[Redacted]**

287. **[Redacted]**

Employment Tribunals

288. Where an employee is dismissed, they may bring proceedings before an Employment Tribunal under the **Employment Rights Act 1996,** the **Race Relations Act 1976,** the **Sex Discrimination Act 1975** or the **Disability Discrimination Act 1995.** The procedure for bringing cases before an Employment Tribunal is as prescribed in the **Employment Tribunals (Constitution and Rules of Procedure) Regulations 2001.** In certain circumstances, proceedings may be bought under the **Race Relations Act** by the Commission for Racial Equality (CRE), under the **Sex Discrimination Act** by the Equal Opportunities Commission (EOC), and under the **Disability Discrimination Act** by the Disability Rights Commission (DRC). Proceedings brought by these bodies should be dealt with in a similar manner to any other proceedings.

289. Under the procedures mentioned above the department will receive a copy of the claimant's originating application and, within 21 days of receiving this, will be required to submit a written notice of appearance. If departments receive an originating application they should refer it to their departmental legal adviser forthwith. It is possible to apply for an extension to this time period. Submission of a written notice of appearance involves the Respondent department stating whether it intends to resist the application and, if so "setting out sufficient particulars to show on what grounds". **Where National Security is at issue, supplemental rules of procedure exist.**

290. Before responding to any proceedings the department should satisfy itself that:

    a. The grounds for the original decision remain valid **[Redacted]**

    b. It is impossible for the individual to be found suitable employment elsewhere; and

    c. The case must be treated as a security matter, rather than as a personnel management matter.

291. Where a department decides that a dismissal has been made on the grounds of health or character then the case should be treated as a management decision and the defence before the Tribunal should not invoke security considerations. If the Tribunal

decides in favour of the complainant it may order his or her reinstatement or reemployment, or the payment of compensation.

292. Where the department, after consideration decides that the case must continue to be treated as a security matter, then it may be appropriate to seek a Ministerial exemption and/or direction on national security grounds. Instructions on how this should be done are different for each Act, and are therefore considered separately below:

Employment Rights Act 1996

293. Section 94 of the **Employment Rights Act 1996** grants a right not to be unfairly dismissed. This includes dismissal of persons in Crown employment, by virtue of section 191. Where it is shown, however, that the action complained of was taken for the purpose of safeguarding national security, section 10(1)b of the **Employment Tribunals Act 1996** states the Tribunal "shall" dismiss the complaint. In matters of Crown employment, where a Minister considers it "expedient in the interests of national security", the minister may direct that:

a. The Tribunal sit in private for all or part of the proceedings;

b. The Tribunal exclude the applicant from all or part of the proceedings;

c. The applicant's representatives be excluded from all or part of the proceedings;

d. The Tribunal take steps to conceal the identity of a particular witness;

e. The Tribunal take steps to keep Secret all or part of the reasons for its decision in particular Crown employment proceedings.

There are no longer provisions that a certificate, issued by a Minister, to the effect that the action complained of was taken for the purpose of national security is conclusive evidence of that fact.

294. If departments consider that security issues are engaged, they should consult departmental legal advisors as soon as possible.

Race Relations Act 1976 (as amended by the Race Relations (Amendment) Act 2000)

295. Cases involving the ***Race Relations Act 1976*** will be more likely to arise at the recruitment stage: where a candidate for clearance is already in employment it is probable that a solution can be found by administrative means. Cases under this Act may be brought through an Employment Tribunal. The Commission for Racial Equality may assist individuals and, in certain circumstances, may itself institute proceedings. In addition, **Section 65** provides a procedure for individuals to obtain information from persons they allege have discriminated against them.

296. Departments defending cases under this Act may invoke **Section 41(1), Section 41 (2)** or **Section 42** of the Act. **Section 41(1)** in effect provides that discrimination is not unlawful if it is performed under statutory authority, such as in connection with Civil Service nationality rules.

297. **Section 41(2)** allows discrimination on the grounds of nationality or place or length of residence under arrangements approved, or conditions imposed, by a Minister. It is nonetheless possible that such discrimination would contravene **Article 48** of the **EC Treaty.**

298. **Section 42** provides that a discriminatory act is not unlawful if it is done for the purpose of national security.

299. **Section 69(2)** provides that a Ministerial certificate may still be issued to the effect that specified arrangements or conditions were in operation at the specified time and is conclusive evidence of the matters certified. If departments consider that the cases they are dealing with is one where a certificate may be required, they should consult departmental legal advisors at an early stage.

Sex Discrimination Act 1975/Sex Discrimination (Amendment) Order 1987

300. Cases involving the ***Sex Discrimination Act*** will be more likely to arise at the recruitment stage: where a candidate for clearance is already in employment it is probable that a solution can be found by administrative means. Cases under this Act may be bought forward through an Employment Tribunal - **refer to paragraph 287** - or through certain civil courts. The Equal Opportunities Commission may assist individuals and, in certain circumstances, may itself institute legal proceedings.

301. Cases involving security clearance may be defended under **Section 51(A)** or, more probably, **Section 52** of the act. **Section 51(A)** provides that discrimination is not unlawful if it is done under the statutory authority; however, in the unlikely event that a case bought under the **Sex Discrimination Act** will involve security clearance, departments would be well advised not to use **Section 51(A)** but instead to rely on **Section 52.**

302. **Section 52** provides that discrimination is not unlawful if it is done for the purpose of safeguarding national security. A defence on the basis of **Section 52** might require a department to produce evidence of the security reasons for the decision. It is therefore important that the Cabinet Office and the departmental legal adviser are informed at the earliest opportunity, if a refusal of clearance is challenged under this Act.

303. Identical security provisions are contained in the **Sex Discrimination (Northern Ireland) Order 1976** as amended by the **Fair Employment and Treatment (Northern Ireland) Order 1998.**

Disability Discrimination Act 1995

304. Under the **Disability Discrimination Act 1995** it is unlawful for an employer to discriminate against a disabled person, whether an employee or an applicant (section 4). Discrimination can take a wide variety of forms, Section 59, however provides that "nothing in this Act makes unlawful any act done for the purpose of safeguarding national security". As stated above in relation to the **Sex Discrimination Act,** a

defence based on section 59 might require a department to produce evidence of the security reasons for the decision. It is important therefore that the Cabinet Office and the departmental legal adviser are informed at the earliest opportunity.

305. The purpose of the **Fair Employment and Treatment (Northern Ireland) Order 1998** is to promote equality of opportunity by making it unlawful to discriminate between people of different political and religious beliefs in connection with employment. The Crown is not exempt from the provisions of the Order. A **Fair Employment Tribunal** and an **Equality Commission for Northern Ireland** exist to hear and oversee complaints brought. Cases involving this Order will be more likely to arise at the recruitment stage: where a candidate for clearance is already in employment it is probable that a solution can be found by administrative means.

306. Departments with employees in Northern Ireland should be aware of the possibility of challenge to vetting decisions under this Order. **[Redacted]**

307. Although the Order binds the Crown, sections 78 and 79 respectively provide that acts done under statutory authority, or to safeguard national security/protecting public safety or public order will not be unlawful providing the "doing of the act is justified by that purpose" (section 79). Whilst there is a mechanism for a Secretary of State to issue a certificate stating that acts specified in the certificate were done for the purpose of safeguarding national security etc, that certificate is no longer conclusive proof and may be challenged by the complainant and quashed by the Tribunal.

308. Section 93 of the **Fair Employment and Treatment (Northern Ireland) Order 1998** gives power to a Minister of the Crown or a Northern Ireland Minister to issue a certificate stating documents and/or information which it is claimed should not be disclosed for the purposes of any investigation, appeal of proceedings under this order. The bases for resisting are that disclosure "would be prejudicial to the safety of the United Kingdom or any part of it or otherwise contrary to the public interest".

309. As soon as it becomes clear that a department may need to issue a Ministerial certificate, the department legal adviser should be consulted. The issue of such a

certificate may lead to a legal challenge by the complainant and subsequent unwelcome publicity. It is therefore important that departments do not enlarge on any security considerations which may have given rise to the issue of the certificate. All these considerations should be made known to the Minister before a certificate is signed.

Data Protection Act

310. An individual's right of access to personal information (data) concerning that individual, is enshrined in the **Data Protection Act**.

311. The Act requires those who hold personal data to register that fact with the Data Protection Registrar, together with a description of the data, its source and the person to whom it may be disclosed. Disclosure to any persons not described in the register is forbidden. **Section 7** of the Act gives the subject of such data the right of access to it.

312. Sensitive personal data held by departments in connection with personnel security may be protected by **Section 28(1)** of the Act, which exempts data from the provisions of the Act dealing with registration and disclosure if the exemption is required for the purpose of safeguarding national security. Under **Section 28(2)** of the Act a Ministerial certificate stating that exemption is so required is conclusive evidence of the fact. Section 28(3) allows for such a certificate to be issued with prospective effect.

313. However, **Section 28(4)** of the Act allows for any person directly affected by the issuing of a certificate under **Subsection (2)** to appeal against it to the Information Tribunal. If the Tribunal finds that the Minister did not have reasonable grounds for issuing the certificate, it may allow the appeal and quash the certificate.

Judicial Review

314. Where an individual feels that he or she has not received adequate redress for a grievance, they may apply to the High Court for Judicial Review of the department's conduct. If Judicial Review proceedings are initiated in a case involving security clearance there will inevitably be a risk of unwelcome publicity. Departments should therefore seek to ensure that decisions on vetting clearance and any subsequent complaints are dealt with in such a way that the possibility of Judicial Review can be avoided, by treating them in as careful and demonstrably fair a manner as possible. Where a case seems likely to proceed to Judicial Review, departments should advise the Cabinet Office as soon as possible.

European Convention on Human Rights and Human Rights Act 1998

315. By enacting the **Human Rights Act 1998** the UK has brought fully into domestic law the **European Convention on Human Rights (ECHR)**. This legislation guarantees to every person in the UK certain human rights and fundamental freedoms including the right to privacy and freedom of expression. These rights are subject to a number of exceptions; in particular they may be subjected to such interference as is necessary in a democratic society in the interests of national security. The extent of an individual's right to privacy and freedom of expression in this context has been tested in the European Court of Human Rights by a number of cases. It is important that in applying the vetting system departments have full regard to the **ECHR**, as interpreted by the European Court. Where it seems possible that a complaint may be brought under the **ECHR**, the Cabinet Office should be consulted at an early stage.

Other relevant legislation

316. At present there is no legislation aimed specifically at the security of computers in the government, public, corporate or private sectors. However, there are several UK statutory provisions that can be applied to computers, their security and the protection of the data stored on them. The following lists the principal Acts, but does not offer full coverage of the legal issues:

    a. ***Computer Misuse Act 1990*** - Makes it an offence to gain access to or modify computer material without authority.

b. ***Wireless Telegraph Act 1949*** - Regulates wireless telegraphy, including by making it an offence to use wireless telegraphy apparatus without authority to intercept messages and to disclose the contents of such messages.

c. ***Regulation of Investigatory Powers Act 2000*** - The main purpose of this Act is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers include the interception of communications, intrusive surveillance and the acquisition of communications data.

d. ***Data Protection Act 1998*** - Regulates the use of automatically processed data and manual data if stored in a "relevant filing system". Departments and agencies should consult their legal advisers for guidance as to the precise scope and application of these Acts.

[Redacted]

317. **[Redacted]**

Overseas Travel

318. Overseas travel can present a variety of security risks. Foreign intelligence services may show an interest in any UK government employees, particularly those with access to valuable government assets or who work in areas involving science or advanced technology (even if not protectively marked). Attempts may be made to approach or compromise them with the intention of recruiting them or using them for intelligence purposes. These risks may be encountered anywhere, since some foreign intelligence services are active against UK interests in all parts of the world, not just in their own countries. The threat from terrorism and local violence is sometimes towards Westerners more generally rather than UK government employees in particular, but UK official representation can be a convenient and high profile target for acts of violence.

[Redacted]

[Redacted]

319. **[Redacted]**

320. **[Redacted]**

[Redacted]

321. **[Redacted]** The Foreign and Commonwealth Office (FCO) provides regularly updated information on countries where terrorism or civil unrest is a potential threat. Travel information is available from the FCO website www.FCO.gov.uk.

[Redacted]

[Redacted]

322. **[Redacted]**

323. Some individuals with access to particularly sensitive assets may require special briefing, or even be subject to particular travel restrictions. It is for departments and agencies, taking into account the threats to their own business and the nature of the access of individuals to sensitive government information, to consider the need for restrictions on private travel by employees, and to bring such restrictions to the attention of those concerned. Individuals holding SC clearance should inform their security department through their line manager, at least ten working days in advance of travel. Employees holding DV clearance should seek written approval at least ten working days in advance of travel.

324. When travel restrictions are imposed, departments and agencies may be required, from time to time, to explain and defend this policy. In such cases, no public comment should be offered as to the countries to which restrictions apply. **[Redacted]**:

[Redacted]

Approving or Refusing Travel Plans

325. When deciding whether or not to approve an individual's travel plans to a country of concern, the following should be taken into account:

a. The assessment of the threat to UK interests from foreign intelligence services operating in the country being visited.

b. The purpose of the visit.

c. The mode of travel.

d. Whether the trip is being arranged independently or is part of a package.

e. Whether the individual is travelling alone or with others.

f. Whether the visa and arrangements, or application for a visa, are likely to draw attention to the individual or their work.

g. The nature and sensitivity of the assets to which the individual has access to, or custody or knowledge of.

326. **[Redacted]**

327. Should employees be involved in a security incident, arrested or approached with a request for information during a foreign trip, a full report to the DSO or Security Controller should always be made. **[Redacted]**

Appendix 1: Prime Minister's Statement on Security Vetting

STATEMENT OF HM GOVERNMENT'S VETTING POLICY

Hansard, 15 December 1994: Written Answers Cols 764-766

Sir Anthony Durant: To ask the Prime Minister if he will make a statement about the procedures for security vetting within government.

The Prime Minister: As I announced to the House on 23 March, Official Report, columns 259-260, to ensure that security measures and procedures reflect current threats, the Government have recently completed a fundamental review of their arrangements for the management of protective security in Departments and Agencies. In the area of personnel security, the review concluded that the vetting process served a worthwhile purpose, not only in disclosing circumstances which might lead to breaches of security but as a deterrent to those who might otherwise seek to undermine that security. The review recommended, however, that there should be a streamlining of the procedures that made up the vetting process. That work has now been completed. The new framework should ensure that personnel security objectives are properly defined and that responsibility for achieving them is clearly established. There will be a greater emphasis on ensuring that personnel security resources are targeted on, and proportionate to, the threat and add necessarily and cost-effectively to the protection of government assets. Between 1 January and 31 March 1995, the existing arrangements will be replaced by a new personnel security regime which will consist of two levels of vetting, a security check and developed vetting. A security check will be similar to the current PV(S) – positive vetting (Secret) – clearance, but will in addition include a check on the financial status of the individual. Developed vetting will replace the present PV(TS) – positive vetting (top Secret) – EPV – enhanced positive vetting – levels of vetting. The current system of counter terrorist checks will remain unchanged, but will be subject to review. As at present, all candidates for security vetting will be asked to complete a security questionnaire which will explain the purpose of the procedure and invited them to provide the personal details for the necessary checks to be carried out. Vetting will then be carried out on the basis of the statement below.

In the interests of national security, safeguarding Parliamentary democracy and maintaining the proper security of the Government's essential activities, it is the policy of HMG that no one should be employed in connection with work the nature of which is vital to the interests of the state who:

- Is, or has been, involved in, or associated with any of the following activities:
    i. Espionage,
    ii. Terrorism,
    iii. Sabotage,
    iv. Actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means; or

- Is, or has recently been :
    i. A member of any organisation which has advocated such activities; or
    ii. Associated with any such organisation, or any of its members in such a way as to raise reasonable doubts about his or her reliability; or

- Is susceptible to pressure or improper influence, for example because of current or past conduct; or

- Has shown dishonesty or lack of integrity which throws doubt upon their reliability; or

- Has demonstrated behaviour, or is subject to circumstances which may otherwise indicate unreliability.

In accordance with the above policy, Government departments and agencies will carry out a **Security Check (SC)** on all individuals who require long term, frequent and uncontrolled access to **SECRET** information or assets. A Security Check may also be applied to staff who are in a position directly or indirectly to bring about the same degree of damage as such individuals or who need access to protectively marked material originating from other countries or international organisations. In some circumstances, where it would not be possible for an individual to make reasonable progress in their career without clearance to **SECRET** level, it may be applied to candidates for employment whose duties do not, initially, involve such regular access.

An SC clearance will normally consist of:

- A check against the National Collection of Criminal Records and relevant departmental and police records;

- In accordance with the Security Service Act 1989, where it is necessary to protect national security, or to safeguard the economic well-being of the United Kingdom from threats posed by persons outside the British Islands, a check against Security Service records; and

- Credit reference checks and where appropriate, a review of personal finances.

  In some circumstances further enquiries, including an interview with the subject, may be carried out.

Individuals employed on government work who have long term, frequent and uncontrolled access to **TOP SECRET** information or assets, will be submitted to the level of vetting clearance known as **Developed Vetting (DV)**. This level of clearance may also be applied to people who are in a position directly or indirectly to cause the same degree of damage as such individuals and in order to satisfy the requirements for access to protectively marked material originating from other countries and international organisations. In addition to a Security Check, a DV will involve:

- An interview with the person being vetted; and

- References from people who are familiar with the person's character in both the home and work environment. These may be followed up by interviews. Enquiries will not necessarily be confined to past and present employers and nominated character referees.

It is also the Government's policy that departments and agencies will carry out **Counter Terrorist Checks (CTC)** in the interests of national security before anyone can be:

- Authorised to take up posts which involve proximity to public figures at particular risk of attack by terrorist organisations, or which give access to information or material assessed to be of value to terrorists;

- Granted unescorted access to certain military, civil and industrial establishments assessed to be at particular risk of attack by a terrorist organisation.

The purpose of such checks is to prevent those who may have connections with terrorist organisations, or who may be vulnerable to pressure from such organisations, from gaining access to certain posts, and in some circumstances, premises, where there is a risk that they could exploit that position to further the aims of a terrorist organisation. A **CTC** will include a check against Security Service records. Criminal record information may also be taken into account.

Departments and agencies generally assure themselves, through the verification of identity, and written references from previous employers, that potential recruits are reliable and trustworthy. Such Basic Checks (BC) are already standard procedure for many departments and agencies. Where access needs to be granted to Government information or assets at **CONFIDENTIAL** level, departments, agencies and contractors engaged on government work are required to complete such checks. In some cases, at the **CONFIDENTIAL** level, where relevant, the Basic Check may be augmented with some of the checks normally carried out for security clearances.

Appendix 2: **[Redacted]**

Appendix 3: **[Redacted]**

Appendix 4: **[Redacted]**

Appendix 5: **[Redacted]**

Appendix 6: **[Redacted]**

Appendix 7: Adjudicative Guidelines

Introduction

1. The following are intended to provide guidance to assessors for assessing the relative relevance, importance and impact of information obtained during the vetting process. They are guidelines only and must not be used as a substitute for judgement or as a checklist. The guidelines should be revisited on a regular basis to ensure that they remain up-to-date and relevant.

Basis of assessment for vetting information

2. Assessment should be based on a balanced judgement of both the positive and negative aspects of the subject. These factors should be weighed against one another and the security requirements of the post in order to reach a sensible conclusion regarding the subject's suitability to handle, be exposed to or be responsible for sensitive information and assets. Over-emphasis on the negative aspects of the subject may lead to risk avoidance rather than risk management.

3. Assessors should remember that they are not passing moral judgement on the subject, and must not allow their judgement to be clouded by moral or cultural preconceptions. The purpose of vetting is to objectively determine the degree to which the subject may present a security risk if employed in a sensitive post.

4. The observation and evaluation of the behaviour and character of the subject by the investigator is the key element in evaluating the personality and traits of the subject. This should be compared both with the information obtained from referees and from the other vetting checks. In support of this, more detailed and specific aggravating and mitigating factors for adverse information are detailed and should be taken into consideration.

5. **[Redacted]**

6. **[Redacted]**:

   a. **[Redacted]**

   b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

j. **[Redacted]**

k. **[Redacted]**

l. **[Redacted]**

m. **[Redacted]**

7. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

d. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

8. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

9. **[Redacted]**

10. **[Redacted]**

[Redacted]

11. **[Redacted]**

[Redacted]

12. **[Redacted]**

13. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

14. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**

    d. **[Redacted]**

[Redacted]

15. **[Redacted]**

16. **[Redacted]**:

    a. **[Redacted]**;

    b. **[Redacted]**;

    c. **[Redacted]**;

    d. **[Redacted]**;

    e. **[Redacted]**;

    f. **[Redacted]**;

    g. **[Redacted]**;

    h. **[Redacted]**;

    i. **[Redacted]**

17. **[Redacted]**:

a. **[Redacted]**;

b. **[Redacted]**;

c. **[Redacted]**;

d. **[Redacted]**;

e. **[Redacted]**;

f. **[Redacted]**;

g. **[Redacted]**;

h. **[Redacted]**

[Redacted]

18. **[Redacted]**

19. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

20. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

[Redacted]

21. **[Redacted]**

22. **[Redacted]**:

a. **[Redacted]**

23. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

[Redacted]

24. **[Redacted]**

25. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

26. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

[Redacted]

27. **[Redacted]**

28. **[Redacted]**

29. **[Redacted]**

30. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

j. **[Redacted]**

31. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

[Redacted]

32. **[Redacted]**

33. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

34. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

[Redacted]

35. **[Redacted]**

36. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

37. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

[Redacted]

38. **[Redacted]**

39. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

40. **[Redacted]**

41. **[Redacted]**

42. **[Redacted]**

43. **[Redacted]**

44. **[Redacted]**

[Redacted]

45. **[Redacted]**

46. **[Redacted]**

47. **[Redacted]**

48. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**

    d. **[Redacted]**

    e. **[Redacted]**

    f. **[Redacted]**

    g. **[Redacted]**

    h. **[Redacted]**

    i. **[Redacted]**.

    j. **[Redacted]**

    k. **[Redacted]**

    l. **[Redacted]**

    m. **[Redacted]**

49. **[Redacted]**:

    a. **[Redacted]**

    b. **[Redacted]**

    c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

h. **[Redacted]**

i. **[Redacted]**

[Redacted]

50. **[Redacted]**

51. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

52. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

[Redacted]

53. **[Redacted]**

54. **[Redacted]**

[Redacted]

55. **[Redacted]**

56. **[Redacted]**

57. **[Redacted]**

58. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

59. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

d. **[Redacted]**

e. **[Redacted]**

f. **[Redacted]**

g. **[Redacted]**

[Redacted]

60. **[Redacted]**

61. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

c. **[Redacted]**

62. **[Redacted]**:

a. **[Redacted]**

b. **[Redacted]**

Appendix 8: Line Managers' Guide

Line manager's guide

1. Line Managers play an important role in ensuring the security of their organisation, particularly in respect of personnel security. Except for personal friends and close colleagues, an individual's line manager is likely to have a more detailed and accurate knowledge of the individual than anyone else in the organisation.

2. It is particularly noteworthy that in many recent espionage cases, both in the UK and overseas, line managers had been aware to some extent, that a security problem had arisen, but had failed to appreciate its significance or had not realised their responsibility for reporting the matter.

Purpose of personnel security

3. The current policy on security vetting, which came into effect on 1 January 1995, was set out in a statement made by the Prime Minister, on 15 December 1994. The statement includes reference to the framework of personnel security controls that must be applied to individuals who, in the course of their work, have access to, or knowledge or custody of, sensitive government information or other valuable assets.

4. The purpose of Personnel Security is to provide an acceptable level of assurance as to the integrity of individuals involved in such work.

5. Security vetting does not provide a guarantee of reliability and trustworthiness. A security clearance is only as good as the background records and other investigations on which it is based at the time the process is carried out. It can never be fully reliable, since individuals and their circumstances change. It must always be an important part of the line manager's responsibility to manage employees in such a way as to minimise security risks.

Personnel security controls

6. Personnel Security aims to provide an acceptable level of assurance as to the integrity of individuals whose work requires them to have access to, or knowledge or custody of, sensitive government information and other valuable assets. Four levels of personnel security controls are available depending on the level of access required:

- **Baseline Standard (BS)**
- **Counter Terrorist Check (CTC)**
- **Security Check (SC)**
- **Developed Vetting (DV)**

7. Of these CTC, SC and DV are formal security clearances obtained through the security vetting procedures, set out earlier. The BS is not a security clearance but aims to provide an appropriate level of assurance as to the trustworthiness and integrity of individuals handling sensitive government assets. In some cases a BS may need to be reinforced with some of the checks used in the formal security clearances.

Personnel security requirements

Responsibilities of line managers

8. Line managers are responsible for good security in their organisations. In respect of personnel security, this means:

a. Setting the security clearance levels, if any, of posts in consultation with their DSO or Security Controller.

b. Briefing and indoctrinating employees.

c. Monitoring subordinates behaviour and, where appropriate, reporting annually on their security performance.

d. Creating a positive climate in which security is given an appropriate priority and individuals are encouraged to discuss concerns before they become security problems.

e. Dealing with problems and reporting any concerns to the DSO or Security Controller.

Setting clearance levels

9. The majority of employees are security cleared without difficulty and throughout their working lives never give the slightest cause for concern. Government departments and agencies and commercial contractors rely on line managers to spot potential difficulties and draw attention to them. Any relevant concerns should be reported to the Departmental Security Officer or the Security Controller, or to a member of their staff.

10. It is usually the responsibility of line managers, in consultation with the DSO or the Security Controller, to decide the personnel security requirements for particular posts and to review those posts at appropriate intervals. They should bear in mind that it is important to assess posts so that individuals are security cleared to appropriate levels consistent with the access they need to sensitive government assets. At the same time, the assessment of posts should take into account that vetting is expensive so over categorisation of posts is both time consuming and wasteful.

11. It is the responsibility of line managers, in consultation with the DSO or Security Controller to review the need for security clearances at suitable intervals, bearing in mind the level of access required in each post.

12. The decision on CTC requirements rests with the DSO, in consultation with senior management, and is usually decided on a site by site basis.

Recruitment and briefing

13. When interviewing an individual for a post, line managers should bring any security aspects of the job to the attention of the candidate, for example, the requirement for and the implications of, a security clearance. The line manager is also responsible for briefing individuals on joining, or when they are moved into a different area of work, about any aspects of the work that might raise issues of security or potential conflicts of interest. In particular they should ensure that any controversial areas of activity, for example, nuclear weapons, animal experiments etc, are highlighted and should try to establish if the individual is content to be involved in that particular type of work.

14. A line manager might be involved in formal special briefings of individuals as a prerequisite for access to particularly sensitive assets. Even outside the most sensitive areas of security, individuals may become worried about aspects of their work which they consider could be interpreted as being against the interests of some sector of society. Where it is known or suspected that an individual has either a negative attitude to security or is unhappy to be involved with that type of work, the line manager should assess the strength of those feelings and, if necessary:

a. Exclude the individual from any final choice of candidates.

b. Seek the advice of the DSO or Security Controller.

c. Decide whether or not the most appropriate action is to monitor the situation for a short period to see how the matter develops.

Monitoring employees

15. Line managers are expected to monitor employees for behaviour which could suggest unreliability or susceptibility to adverse pressure. They should look out for certain types of behaviour - **refer to paragraph 21**. Particular attention should be made to individuals under 21 years old, whose character will still be forming and to those who might be

willing to talk matters over but who are clearly unhappy, have few friends and appear to be alienated from colleagues. Experience has shown the latter type of individual is more likely to act in an erratic way to the detriment of the organisation. When monitoring individuals, it is very important that line managers maintain a sense of perspective. It is not the intention that line managers should spy on individuals, set traps for them or adopt a censorious approach with regard to their personal lives.

Discussing concerns

16. It is unusual for serious security problems to arise with staff who feel able to express themselves freely and can approach a line manager about problems. It is important that line managers create an atmosphere in which staff can feel confident that there will always be a sympathetic ear to any matter which they consider might have a bearing on security. It should be emphasised that such matters will be treated in confidence and discussed, if necessary, only with the DSO or Security Controller and their staff. A sympathetic approach is far more likely to achieve the cooperation of staff, and is essential if good security practices are to be maintained.

Dealing with problems

17. Where an individual has expressed security concerns, the line manager will need to decide if the concern is of security significance. Where the information is of no serious concern, reassurance and advice should be offered. Where the matter appears to be serious or its significance is unclear, the DSO or Security Controller should be consulted before taking any further action.

18. Should a line manager receive security allegations about an individual or about someone elsewhere in government service, regardless of seniority, it should reported to the DSO or Security Controller unless it is clear that the story is ill-founded or malicious. The DSO or Security Controller will not assume that any allegation is true without taking steps to verify what has been reported or seeking the advice of other departments or agencies. It is important that all allegations of a security nature are resolved, one way or the other, for the sake of all concerned. An atmosphere of doubt and suspicion is likely to demoralise a workforce. Failure to take seriously a complaint relating to security could

tempt someone to leak information as the only means of getting the matter taken up at a higher level.

19. Any concerns about a possible security problem involving an individual should be reported to the DSO or Security Controller at the earliest opportunity, with a view to getting expert advice. They will, if necessary and in confidence, consult relevant parties outside the department, agency or company, before deciding what action to take. Line managers should not feel that a 'no action' response is seen as a bad reflection on them. It is far better that the DSO or Security Controller is alerted unnecessarily rather than ignoring a genuine security problem.

20. Where a security problem is dealt with in the early stages, it is often possible to resolve the matter without jeopardising the individual's career, for example, moving the individual to other work or arranging counselling. Where the matter is neglected the consequences could be serious for both the individual concerned and for the department, agency or company.

Vulnerability and personnel security problems

Areas of vulnerability

21. Line managers should be aware of the circumstances and of behaviour which could render staff susceptible to pressure or improper influence, or could otherwise indicate unreliability. Some of the more obvious are:

a. Financial problems

b. Drug abuse

c. Alcohol abuse

d. Sexual misconduct*

e. Illegal or injudicious behaviour particularly when living or travelling overseas.

f. Compulsive gambling

g. Involvement with extreme political groups, that is, those involved in or advocating espionage, terrorism, sabotage or actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means.

* It is government policy that homosexual behaviour by either sex should not of itself bar a person from obtaining security clearance. In general, as long as there is no attempt to conceal the matter and the individual's behaviour does not indicate indiscretion or unreliability, there should be no problem.

Signs of personnel security problems

22. Although it is difficult to discover if an individual poses a threat to security, past experience shows that certain warning signs can be detected. Single instances of the type of behaviour described below may be of little or no significance. But, the presence over a period of time of several of these signs could indicate a serious problem.

23. When considering what appears to be a potential security problem managers should take into account individual and cultural differences. What might be considered a potential danger signal in one person might be relatively normal for another. In some cases there may be only a hint of a potentially serious security problem and some signs are more obvious when an individual is under pressure. The following examples apply to staff of all ages and illustrate some of the points line managers should be on the look out for:

a. Change in personality, for example, from gregarious to withdrawn.

b. Worsening attendance record, for example, frequent self-certificated sick leave.

c. Falling off of performance, for example, uncharacteristic tendency to make mistakes or commit security breaches.

d. Signs of drug or alcohol abuse - **refer to paragraph 24**.

e. Minor acts of dishonesty.

f. Change in pattern of working hours, particularly when this will mean that the individual will be able to spend significant periods of time alone in an area of a building or site where access to protectively marked assets would be possible.

g. Tendency to become accident-prone.

h. Marked changes in lifestyle, for example, unexplained affluence or debt.

i. Marked change in appearance, particularly a decrease in attention to personal hygiene and tidiness.

Signs of drug and alcohol abuse

24. Some of the signs and symptoms described below, when taken in isolation, may be of no significance, or may be due to illness. When several appear together, they could

indicate drug or alcohol abuse. Unless the matter is clearcut, the line manager should try to discuss the situation informally and sympathetically with the individual, with the aim of finding out what lies at the root of the problem. This should be done before consulting the DSO or Security Controller. Even if the DSO or Security Controller does not need to involved, it may still be appropriate to refer the individual to welfare, medical or counselling services.

Drug abuse

25. The following are possible signs of drug abuse:

a. An apparent change in personality or general attitude, for example, to family, colleagues or work.

b. Unexplained inadequate or uneven performance, particularly when indicated by erratic timekeeping or disregard for discipline.

c. Personality changes such as:

i. Furtive behaviour
ii. Stealing
iii. Frequent attempts to borrow money
iv. Obvious familiarity with slang expressions for drugs and methods for taking them

d. Wearing sunglasses in inappropriate conditions - some illegal drugs contract or dilate the pupils of the eye to a marked extent.

e. Attempts to keep arms covered, even in hot weather, to hide needle marks.

f. Unexplained absences during the working day - to provide the opportunity to take illegal drugs in private.

Alcohol abuse

26. The following are possible signs of alcohol abuse:

a. Inadequate or uneven performance at work particularly indicated by:

i. A lack of concentration or loss of interest
ii. Afternoon lethargy
iii. Unexplained absences during the working day
iv. Unreliability and forgetfulness
v. Reluctance to accept responsibility or over sensitivity to criticism
vi. Poor timekeeping

b. Physical deterioration, such as:

i. Bleary eyes, slurred speech, flushed face, unsteadiness or hand tremors
ii. Smell of alcohol on the breath in the morning
iii. Frequent sick leave, explained as minor illness, especially when it occurs often on Monday mornings

c. personality changes such as:

i. Moodiness
ii. Anxiety
iii. Depression
iv. Aggressiveness.

Appendix 9: **[Redacted]**

Appendix 10: **[Redacted]**

Appendix 11: **[Redacted]**

Appendix 12: **[Redacted]**

THE GOVERNMENT SECURE INTRANET

CODE OF PRACTICE

THIS CODE OF PRACTICE is entered into on the day of …… 20

BY:

(1) [*** ***] ("the CUSTOMER"); and

(2) the Lords Commissioners of Her Majesty's Treasury as represented by Buying Solutions being a separate Trading Fund of Her Majesty's Treasury without separate legal personality ("the AUTHORITY")

WHEREAS:

a) the AUTHORITY has entered into a Framework Agreement with Energis Communications Limited, a C&W group company, whose registered office is at Waterside House, Longshot Lane, Bracknell, Berks, RG12 1XL, and whose registered number is 2630471 ("the CONTRACTOR") for the provision of Government Secure Intranet Services;

b) the CUSTOMER wishes to gain access to the Services (as defined in Appendix 1) under the terms of a Service Contract;

c) the AUTHORITY has agreed to allow the CUSTOMER to gain access to the Services in certain Service Categories (as defined in Appendix 1) and to allow other public authorities to access those Services via an aggregating gateway to be provided by an external contractor;

d) the CUSTOMER has given details pertinent to the CUSTOMER organisation at Appendix 6; and

e) the parties agree to comply with their respective obligations in this Code of Practice.

IT IS HEREBY AGREED (without intending to create legal relations) as follows:

1. Interpretations.

1.1. As used in this Code of Practice:

1.1.1. the terms and expressions set out in Appendix 1 shall have the meanings ascribed therein;

1.1.2. the masculine includes the feminine and the neuter; and

1.1.3. the singular includes the plural and vice versa.

1.2. A reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment thereof.

1.3. Headings are included in this Code of Practice for ease of reference only and shall not affect the interpretation or construction of this Code of Practice.

1.4. References to Terms and Appendices are, unless otherwise provided, references to terms of and appendices to this Code of Practice.

1.5. In the event and to the extent only of any conflict between the Terms and the Appendices, the Terms shall prevail.

2. Scope of this Code of Practice

2.1. This Code of Practice establishes the terms and conditions that apply to the provision of the Services to the CUSTOMER and specifies the roles and responsibilities of the CUSTOMER and the AUTHORITY.

2.2. The CUSTOMER is entitled (but not required) at any time during the term of this Code of Practice to order Services under certain Service Categories from the CONTRACTOR in accordance with the Ordering Procedures and to provide or procure the provision of Services to other public authorities by an Aggregating GSi Gateway and the CONTRACTOR shall provide such Services in accordance with all applicable provisions of the Service Contract.

2.3. **This Code of Practice relating to the relationship between the AUTHORITY and the CUSTOMER is not intended and shall not be construed to be a legally enforceable agreement or to create legal obligations between the parties or to impose any legal liability whatsoever.** For the avoidance of doubt, the parties acknowledge that use of the terms “party” and “parties” herein is for convenience

only, and is not intended and shall not be construed to establish or imply a separate legal identity for the AUTHORITY or the CUSTOMER.

2.4. The GSi Code of Practice is the customer access agreement specific to GSi.

3. Ordering Procedures

3.1. The CUSTOMER shall be entitled at any time during the term to order Services under the Service Categories authorised by the AUTHORITY. Such Services shall be provided by the CONTRACTOR pursuant to a Service Contract entered into by the CUSTOMER serving an Order on the CONTRACTOR for the supply of such Services in accordance with the Ordering Procedures specified in Appendix 2.

4. Responsibilities

4.1. The AUTHORITY shall perform the AUTHORITY's Responsibilities.

4.2. The CUSTOMER shall perform the CUSTOMER's Responsibilities.

5. Provision of Information

5.1. The CUSTOMER shall promptly notify the AUTHORITY of any changes that may become necessary to the information set out in Appendix 6.

6. Warranties and Representations

6.1. The CUSTOMER warrants and represents that the CUSTOMER has full capacity and authority and all necessary consents to enter into and to perform this Code of Practice and that this Code of Practice is executed by the duly authorised representatives of the CUSTOMER.

7. Confidentiality

7.1. Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the CUSTOMER acknowledges that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

7.2. Both parties hereby warrant that:

7.2.1. any person employed or engaged by the parties (in connection with this Code of Practice in the course of such employment or engagement) shall only use Confidential Information for the purposes of this Code of Practice;

7.2.2. any person employed or engaged by either the CUSTOMER or the AUTHORITY (in connection with this Code of Practice in the course of such

employment or engagement) shall not disclose any Confidential Information to any third party without the prior written consent of the other party;

7.2.3. both parties shall take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (save as aforesaid) or used other than for the purposes of this Code of Practice by their employees, servants, agents or sub-contractors; and

7.2.4. without prejudice to the generality of the foregoing neither party nor any person engaged by them whether as a servant or a consultant or otherwise shall use the Confidential Information for the solicitation of business from the other or by their servants or consultants or by any third party.

7.3. The provisions of Terms 7.1 and 7.2 shall not apply to any information which:

7.3.1. is or becomes public knowledge other than by breach of this Term 7; or

7.3.2. is in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party; or

7.3.3. is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure; or

7.3.4. is independently developed without access to the Confidential Information.

7.4. Nothing in this Term 7 shall be deemed or construed to prevent the AUTHORITY from disclosing any Confidential Information obtained from the CUSTOMER:

7.4.1. to any other department, office or agency of Her Majesty's Government, provided that the AUTHORITY has required that such information is treated as confidential by such departments, offices and agencies, and their servants or agents, including requiring servants or agents to enter into a confidentiality undertaking where appropriate; and

7.4.2. to any consultant, other customer in receipt of the Services, or other person engaged by the AUTHORITY in connection herewith, provided that the AUTHORITY shall have obtained from the consultant, CUSTOMER or other person a signed confidentiality undertaking on substantially the same terms as are contained in this Term 7.

7.5. Nothing in this Term 7 shall prevent the CUSTOMER or the AUTHORITY from using data processing techniques, ideas and know-how gained during the performance of this Code of Practice in the furtherance of its normal business, to the extent that this

does not relate to a disclosure of Confidential Information or an infringement by the AUTHORITY or the CUSTOMER of any Intellectual Property Right.

8. Term

8.1. This Code of Practice shall commence on the date of execution hereof and shall remain in force for a period of six (6) Months after the expiry or early termination of the Framework Agreement.

9. Termination

9.1. The AUTHORITY may at any time by notice in writing terminate this Code of Practice forthwith if the CUSTOMER is in Default of any obligation under this Code of Practice and:

9.1.1. the Default is capable of remedy and the CUSTOMER shall have failed to remedy the Default within thirty (30) days of written notice to the CUSTOMER specifying the Default and requiring its remedy; or

9.1.2. the Default is not capable of remedy.

9.2. Termination in accordance with this Term 9 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to either party.

9.3. The provisions of Terms 1, 6, 7, 10.2 and 14 and the provisions of Appendix 1 shall survive the termination of this Code of Practice.

10. Protection of Personal Data

10.1. The CUSTOMER's attention is hereby drawn to the Data Protection Act 1998.

10.2. Both parties warrant that they will duly observe all their obligations under the Data Protection Act 1998 and any associated legislation that arises in connection with this Code of Practice.

11. Transfer and Sub-contracting

11.1. This Code of Practice is personal to the CUSTOMER. The CUSTOMER shall not assign, novate, sub-contract or otherwise dispose of this Code of Practice or any part thereof without the previous consent in writing of the AUTHORITY.

12. Amendments to this Code of Practice

12.1. This Code of Practice shall not be varied or amended unless such variation or amendment is agreed in writing by a duly authorised representative on behalf of the AUTHORITY and by a duly authorised representative of the CUSTOMER on behalf of the CUSTOMER.

13. Communications

13.1. Except as otherwise expressly provided, no communication from one party to the other shall have any validity under this Code of Practice unless made in writing by or on behalf of the AUTHORITY or as the case may be by or on behalf of the CUSTOMER.

13.2. Any notice or other communication whatsoever which either party hereto is required or authorised by this Code of Practice to give or make to the other shall be given or made either by post in a prepaid letter, or by email or by facsimile transmission confirmed by post in a prepaid letter, addressed to the other party at the address specified in Appendix 5 and if that letter is not returned as being undelivered that notice or communication shall be deemed for the purposes of this Code of Practice to have been given or made after two (2) Working Days, for a letter, or four (4) Working Hours, for an email or facsimile transmission.

14. Entire Agreement

14.1. This Code of Practice constitutes the entire understanding between the parties relating to the subject matter of this Code of Practice and, save as may be expressly referred to or referenced herein, supersedes all prior representations, writings, negotiations or understandings with respect hereto.

IN WITNESS WHEREOF, the parties hereto have signed this Code of Practice.

Signed for and on behalf of the CUSTOMER

By : **……..**

Name : **……..**

Title : **……..**

Organisation: **……..**

Date : ……..

Signed for and on behalf of the AUTHORITY (Buying Solutions)

By : **……..**

Name : **……..**

Title : **……..**

Date : **……..**

APPENDIX 1

DEFINITIONS

The expressions set out below shall have the meanings ascribed thereto:

“Aggregating Contractor”	means a service provider engaged by an Aggregating Customer to operate the Aggregated GSi Gateway;
“Aggregating Customer”	means a CUSTOMER that is providing customers with the benefits of a GSi connection by connecting or procuring the connection of those customers to an Aggregated GSi Gateway.
“Aggregated Customer”	means a customer connected to an Aggregated GSi Gateway.
“Aggregated GSi Gateway”	means a telecommunications system, other than the GSi, which enables customers to access the Services through their connection to that system.
“AUTHORITY”	means The Lords Commissioners of Her Majesty's Treasury as represented by Buying Solutions being a trading fund of her Majesty's Treasury without separate legal personality.
“AUTHORITY's Responsibilities”	means the responsibilities, listed in Appendix 3, of the AUTHORITY.
“Code of Connection”	means the code setting out the technical and security requirements and other obligations in respect of connection to the GSi
“Code of Practice”	means this agreement, comprised of the Terms and the Appendices hereto.
“Confidential Information”	means all information designated as such by either party in writing, together with all other information which relates to the business, affairs, developments, trade secrets, know-how, personnel, customers and suppliers of either party or information which may reasonably be regarded as the confidential information of the disclosing party.
“Contracting Entity”	means any UK contracting authority and any UK contracting entity (as defined in EC Directives 92/50/EEC and 93/38/EEC respectively and any subsequent legislation).
“CONTRACTOR”	means Energis Communications Limited, a C&W group company.
“CUSTOMER”	means the body identified as the “CUSTOMER” in Appendix 6.
“CUSTOMER's	means the responsibilities, listed in Appendix 4, of the

Responsibilities”	CUSTOMER.
“CUSTOMER User”	means a User that may be expected to be under the reasonable control of the CUSTOMER.

“Default”	means any breach of the obligations of either party (including but not limited to fundamental breach or breach of a fundamental term) or any default, act, omission, negligence or statement of either party, its employees, agents or sub-contractors in connection with or in relation to the subject matter of this Code of Practice and in respect of which such party is liable to the other.
“Framework Agreement”	means the framework agreement between the AUTHORITY and the CONTRACTOR dated 23 August 2003 under which the AUTHORITY has established a contractual vehicle for the provision of the Services subject to Service Contracts.
“GSi”	means the Government Secure Intranet.
“Intellectual Property Rights”	means patents, trade marks, service marks, design rights (whether registrable or otherwise), applications for any of the foregoing, copyright, know-how, trade or business names and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom).
“Month”	means a calendar month.
“Order”	means an order for Services in accordance with the provisions of Appendix 2 served by the CUSTOMER on the CONTRACTOR in accordance with the Ordering Procedure.
“Ordering Procedures”	means the ordering procedures as specified in Appendix 2 to be followed by the CUSTOMER in relation to the serving of an Order on a CONTRACTOR.
“Register of Services” (“RoS”)	means the register of services made available by the CONTRACTOR to customers which forms part of the Framework Agreement. The Register of Services specifies the Services available to customers under Service Contracts, subject to Service Usage Rules for the Specific Services. The RoS is the catalogue of services specific to the GSi.
“Service Categories”	means the service categories listed in the Register of Services from which the CUSTOMER is authorised by the AUTHORITY to Order Services. The Service Categories are: currently Restricted; Restricted High; and Confidential.

“Service Contract”	means a contract to the same terms as those in the Specimen Service Contract for the provision of Services by the CONTRACTOR to the CUSTOMER, entered into by the CUSTOMER serving an Order on the CONTRACTOR.
“Service Usage Rules”	means the service usage rules in respect of each of the Services as specified in the Register of Services.
“Services”	means any of the services, specified in the Register of Services, to be provided under a Service Contract by the CONTRACTOR.
“Specimen Service Contract”	means the specimen service contract included in the Register of Services.
“User”	means an individual that may have access to, or be a direct or indirect recipient of, the Services.
“Working Day”	means Monday to Friday inclusive, excluding English public and bank holidays.
“Working Hours”	means the period between 0730 hours and 1800 hours on Working Days.

APPENDIX 2

ORDERING PROCEDURES

1. Introduction

1.1. This Appendix 2 details the procedure to be adopted by CUSTOMERS in placing Orders for Services with the CONTRACTOR.

2. Authorisation

2.1. Following the execution of this Code of Practice, a copy will be sent by the AUTHORITY to the CONTRACTOR. This will signify the AUTHORITY's authorisation of the CUSTOMER to place Orders for Services within certain Service Categories.

3. Browsing the Register of Services

3.1. The CUSTOMER, when authorised to place Orders, may access the Register of Services at http://gsi.cw.com

3.2. The CUSTOMER may place an Order for Services, following the instructions on the web site, by specifying the Service required and supplying the relevant details necessary for the provision of that Service.

4. Service Contract

4.1. Using the details supplied by the CUSTOMER pursuant to paragraph 3.2 and the CUSTOMER details specified in Appendix 6, the CONTRACTOR will produce a Service Contract. Such Service Contract will be sent by the CONTRACTOR to the CUSTOMER addressee specified in Appendix 5 for execution.

4.2. Upon execution and return to the CONTRACTOR, the Service Contract will be performed by the CONTRACTOR.

APPENDIX 3

AUTHORITY'S RIGHTS AND RESPONSIBILITIES

1. Introduction

1.1. This Appendix 3 sets out the responsibilities of the AUTHORITY hereunder.

2. Scheduled Duties

2.1 The AUTHORITY will undertake the following scheduled activities:

2.1.1 agree changes to the Register of Service with the CONTRACTOR;

2.1.2 approve organisations for connection to the GSi where appropriate;

2.1.3 approve customers for particular Service Categories where appropriate;

2.1.4 assess value for money of GSi Services;

2.1.5 benchmark GSi services;

2.1.6 chair service review meetings with the CONTRACTOR and customers, including the CUSTOMER;

2.1.7 consult the CUSTOMER about Service Usage Rules;

2.1.8 contract management;

2.1.9 deal with questions from EU, National Audit Office, parliament and other bodies about GSi;

2.1.10 introduce arrangements for a new GSi service on expiry of the Framework Agreement;

2.1.11 issue GSi notices;

2.1.12 manage contract change control;

2.1.13 maintain lists of CUSTOMER representatives, and other contacts;

2.1.14 market and promote the take up, use and benefits of GSi; and

2.1.15 oversee security management of GSi with its security partners.

3. Ongoing Duties

3.1. The AUTHORITY will provide a GSi service management team, available via its corporate service desk, to:

3.1.1. advise the CUSTOMER whether prospective services are within the scope of the GSi;

3.1.2. advise the CUSTOMER about contractual issues such as Service Levels, Service Credits and changes in Charges;

3.1.3. approve domain names;

3.1.4. co-ordinate central agreement of changes and maintenance schedules;

3.1.5. escalate faults not resolved by the CUSTOMER and the CONTRACTOR;

3.1.6. escalate faults that impact many customers;

3.1.7. liaise with the European Union with respect to European networking;

3.1.8. liaise with other UK public sector network authorities, e.g. the NHS;

3.1.9. process applications for security accreditation, approval, lodging & review;

3.1.10. publish the central GSi intranet web page;

3.1.11. coordinate exit arrangements from the GSi;

3.1.12. promote the GSi throughout the public sector;

3.1.13. manage and implement the Charges variation mechanism with the CONTRACTOR;

3.1.14. resolve any disputes that may arise; and

3.1.15. work with the CONTRACTOR to resolve service problems.

4. Exceptional Rights and Duties

4.1. The AUTHORITY shall have the right, in its absolute discretion to instruct the CONTRACTOR to:

4.1.1. disconnect the GSi from the Aggregated GSi Gateway;

4.1.2. disconnect the CUSTOMER from the GSi; or

4.1.3. suspend the provision of the Services to the CUSTOMER if it considers that the disconnection or suspension is necessary or desirable to protect the security or integrity of the GSi. If the AUTHORITY exercises this right it shall inform the CUSTOMER of this in writing within two Working Days after the instruction has been given.

4.2. The AUTHORITY shall have the right in its absolute discretion to instruct the CUSTOMER to procure the disconnection of any of its Aggregated Customers from the GSi or the suspension of the provision of the Services to any of its Aggregated Customers if it considers that such disconnection or suspension is necessary or desirable to protect the security or integrity of the GSi. If the Authority exercises this right it shall confirm this in writing to the Aggregated Customer within two Working Days after the instruction is given.

4.3. The AUTHORITY reserves the right not to give any reason as to why any such instruction was given.

APPENDIX 4

CUSTOMER'S RESPONSIBILITIES

1. Introduction

1.1. The obligations in this Appendix 4 are in addition to the CUSTOMER's other obligations that will arise as a result of executing a Service Contract with the CONTRACTOR.

2. Service Usage Rules

2.1. The CUSTOMER shall comply with all applicable Service Usage Rules.

3. CUSTOMER Duties

3.1. The CUSTOMER agrees to

3.1.1. abide by this Code of Practice;

3.1.2. ensure that CUSTOMER Users comply with the obligations set out in paragraph 4 of this Appendix 4;

3.1.3. procure that any Aggregated Customers of the CUSTOMER enter into codes of practice on equivalent terms to this Code of Practice and the Code of Connection, before such Aggregated Customers are permitted to access the Services and that they comply with the Code of Practice and the Code of Connection for as long as they have access to the Services.

3.2. The CUSTOMER is responsible for obtaining and maintaining their accreditation or certification for those Services for which accreditation or certification is applicable.

3.3. The CUSTOMER will not place any Service Contracts for non standard GSi packages i.e. other than as specified in the Register of Services. The CUSTOMER should first liaise with the AUTHORITY about variant GSi requirements so that the AUTHORITY can confirm they are in scope and introduce them by change control.

3.4. the AUTHORITY may obtain or compile any sensitive information about the CONTRACTOR's performance of the Services and supply it to the CUSTOMER. The CUSTOMER agrees to keep such information as confidential and, if passing the information on, to cascade such confidentiality undertaking to its own contractors.

3.5. The CUSTOMER agrees to obtain the specific consent from the AUTHORITY or from the CONTRACTOR, prior to permitting the disclosure of such information to any competitors of the CONTRACTOR.

3.6. The CUSTOMER will notify the AUTHORITY of any change of the CUSTOMER's representative specified in Appendix 6.

3.7. The CUSTOMER will complete and return the CUSTOMER domain details form as issued periodically by the AUTHORITY.

3.8. If the CUSTOMER populates the GSi directory, or grants access from the GSi directory to an internal CUSTOMER directory, the CUSTOMER must update the directory entries at least every Month to minimise any misdirection of classified information that might arise from staff changes and to enable key staff to be contacted urgently as required and for the benefit of other CUSTOMERs.

3.9. The CUSTOMER agrees to accept the AUTHORITY's role and rules for domain name services for:

3.9.1. x.gsi.gov.uk: up to and including protectively marked CONFIDENTIAL;

3.9.2. gsi.gov.uk: up to and including protectively marked RESTRICTED; and

3.9.3. gsx.gov.uk: up to and including protectively marked RESTRICTED;

3.9.4. gcsx.gov.uk: up to and including protectively marked RESTRICTED;

if recipients are cleared to receive such information, and for any other new domain names that may be introduced for GSi.

3.10. The CUSTOMER agrees to cooperate with any investigation into any:

3.10.1. inappropriate disclosure of information;

3.10.2. use not in accordance with public policy; or

3.10.3. criminal activity;

that might be conducted by the AUTHORITY or the appropriate authorities.

3.11. In the event of a national emergency, various business continuity scenarios and/or unforeseen congestion; the CUSTOMER will implement a reduction in demand, including technical measures and issuing instructions to its users, as requested by the AUTHORITY.

3.12. The CUSTOMER agrees that, for any address allocated to it from the domain name ranges in paragraph 3.9; it will not

3.12.1. allow the address to be used by another organisation as a source from address; and

3.12.2. it will not generate emails with such addresses as source from addresses outside of a GSi Community.

3.13. The CUSTOMER undertakes to include in any contract with any Aggregating Contractor, provisions requiring the Aggregating Contractor to:

3.13.1. take such steps as may be required by paragraph 7.1 of this Appendix 4;

3.13.2. monitor, control and report to the AUTHORITY all risks to the security and integrity of the GSi as a result of the GSi's connection to the Aggregated GSi Gateway, and any breaches or apprehended breaches of the Code of Connection by any customer; and

3.13.3. comply with the Code of Connection.

4. CUSTOMER User Duties

4.1. The CUSTOMER agrees to ensure that CUSTOMER Users will abide by the relevant Service Usage Rules.

4.2. CUSTOMER Users are responsible for taking care to ensure that classified information is distributed only on a need to know basis.

4.3. CUSTOMER Users are responsible for taking due care in;

4.3.1. addressing emails;

4.3.2. publishing on the internet and the intranet; and

4.3.3. any use of file transfer protocol,

to ensure that classified information is not inadvertently emailed or otherwise downloaded to a security regime lower than is appropriate for holding the information.

4.4. CUSTOMER Users are responsible for taking care to ensure that classified information is not inadvertently emailed or otherwise transmitted via an insecure regime such as the Internet unless an approved form of encryption is used.

4.5. CUSTOMER Users are responsible for using the appropriate address structure, as specified in paragraph 3.9, to ensure that information remains within the appropriate community.

4.6. CUSTOMER Users must not use the Services for defamatory, offensive, pornographic, racist, sexist, violent or other inappropriate communication purposes.

4.7. CUSTOMER Users shall be responsible for the protection of any authentication materials, including usernames, passwords, PINs and digital certificates, and shall not provide or disclose such authentication materials to unauthorised parties.

5. CUSTOMER Acknowledgements

5.1. The CUSTOMER acknowledges that in the event of the AUTHORITY permitting the CUSTOMER or any Aggregated Customer to Order Services in advance of the CUSTOMER or Aggregated Customer having fully complied with any relevant Service Usage Rules (such as entering into the Code of Connection and obtaining security accreditation), the CONTRACTOR will not enable such Services until the AUTHORITY has given its approval. In such circumstances, the CUSTOMER will still be liable to pay the CONTRACTOR from the ready for service date for that Service Contract, even if the Service has not been activated/enabled.

5.2. In the interests of protecting the communities, ensuring best practice and government policy, the CUSTOMER acknowledges that in the event of any persistent or serious breach of the Service Usage Rules or Code of Connection by the CUSTOMER or any Aggregated Customer, the provision of the relevant Service to the CUSTOMER or Aggregated Customer may be suspended or the Aggregated GSi Gateway may be disconnected. In such circumstances, the CUSTOMER will remain liable for paying the CONTRACTOR during the period of suspension.

5.3. The CUSTOMER acknowledges that in the event of any persistent or serious breach of this Code of Practice, the AUTHORITY may revoke the CUSTOMER's or the relevant Aggregated Customer's status as an approved GSi CUSTOMER.

5.4. The CUSTOMER acknowledges that scheduled maintenance periods for Services impacting upon many or all customers may be agreed between the AUTHORITY and the CONTRACTOR. The AUTHORITY will ensure that advance notice is given of such scheduled maintenance whenever possible.

5.5. The CUSTOMER acknowledges that where it is necessary to temporarily suspend a Service in its entirety for maintenance, the AUTHORITY may collectively agree the date and time of such suspension with the CONTRACTOR. The AUTHORITY will ensure that advance notice is given of such suspension whenever possible.

5.6. The CUSTOMER agrees to accept the AUTHORITY's decisions about the prioritisation of customers and the prioritisation of Services that may arise in addressing business continuity concerns.

6. Aggregated CUSTOMER Acknowledgements

6.1 The CUSTOMER acknowledges and shall procure that each Aggregated Customer shall acknowledge that, where the Aggregated Customer's connection to the GSi and to Services are by means of an Aggregated GSi Gateway:

6.1.1 in the event of the Aggregated Customer's non compliance with this Code of Practice or the Code of Connection, the Aggregated Customer's connection may, upon instruction from the AUTHORITY, be suspended or disconnected;

6.1.2 the Aggregated Customer's connection may, upon an instruction from the AUTHORITY, be suspended or disconnected in the event of the Aggregating Customer's non compliance with the Codes of Connection or Practice by the suspension or disconnection of the Aggregating customer's GSi Connection;

6.1.3 the Aggregated Customer's connection may, upon an instruction from the AUTHORITY, be suspended or disconnected in the event of the non-compliance of another Aggregated Customer of the same Aggregated GSi Gateway with the GSi Codes of Connection or Practice, which the AUTHORITY considers as causing a threat to the security of the GSi and it not being practical to otherwise separately isolate that other Aggregated Customer;

6.1.4 any such disconnection or suspension may, depending upon the technical nature of the aggregating network, adversely impact upon its receipts of services other than GSi Services from the Aggregating Customer; and

6.1.5 no Aggregated Customer shall be permitted to act as an Aggregating Customer (except when it is aggregating for itself, and save insofar as the CUSTOMER acts as both Aggregated Customer and an Aggregating Customer in accordance with its obligations under this Code of Practice).

6.2 The Aggregated Customer acknowledges that the AUTHORITY accepts no liability to the Aggregated Customer for any such disconnection or suspension, regardless of whether this resulted from that Aggregated Customer's default, act or omission.

7. Aggregating CUSTOMER's Additional Acknowledgements

7.1 The CUSTOMER agrees that, where it functions as an Aggregating Customer, in the event of non compliance with the GSi Code of Connection or the GSi Code of Practice by an Aggregated Customer, the CUSTOMER will, upon instruction from the AUTHORITY, procure the suspension of the Services to that Aggregated Customer or the disconnection of that Aggregated Customer from the GSi.

7.2 The CUSTOMER agrees that, if it fails to comply with GSi Codes of Connection or Practice or if it fails to or it is unable to isolate a non compliant Aggregated Customer as in paragraph 7.1, the CONTRACTOR will, upon instruction from the AUTHORITY, suspend the provision of GSi Services to the Aggregated Customer or disconnect the Aggregating Customer from the GSi.

7.3 The Aggregating Customer acknowledges that the AUTHORITY hereby excludes all liability to Aggregating or Aggregated Customers for any claims arising from any such disconnection or suspension of service irrespective of the default or omission of any party.

APPENDIX 5

ADDRESSES FOR SERVICE OF NOTICES

1. Introduction

1.1. This Appendix 5 sets out the addresses of the parties for the service of notices in accordance with the provisions of Term 13.

1.2. Unless otherwise previously agreed in writing by the parties, the service of notices by either party to addresses other than those set out herein shall not be valid hereunder.

2. For the AUTHORITY:

Name:	The GSi Contract Manager
Address:	Buying Solutions Rosebery Court St Andrews Business Park Norwich NR7 0HS
Email address:	GSi@buyingsolutions.gsi.gov.uk
Telephone Number:	0845 410 2222
Fax Number:	01603 704921

3. For the CUSTOMER:

Name:	[ ]
Address:	[ ] [ ] [ ] [ ] [ ]
Email address:	[ ]
Telephone Number:	[ ]
Fax Number:	[ ]

This address is also, by default, the address to which the CONTRACTOR will send Service Contracts for execution.

APPENDIX 6

CUSTOMER DETAILS

	Notes	
Contracting entity (for any Service Contract(s))	e.g. “The Secretary of State for Defence”	
Address for Service of Notices	As required for and in Schedule 17-11 (of the Service Contract).	Please ensure Appendix 5 is completed!
Address for Submission of Invoices	As required for and in Schedule 17-8 (of the Service Contract).	Name Address Tel. No.
Applicable law (specify one only)	English	
	Northern Ireland	
	Scots	
Legal status (specify one only)	Crown	
	Non-Crown	
	Private Authority	
Access to Ministry of Defence (MOD) Sites	Is optional Service Contract MOD Term required?	
Applicant Organisation (the Customer)		Name Address Tel. No. Fax No. Email

CUSTOMER's Representative	To act as single point of contact with the CONTRACTOR	Name Job Title
Members of staff authorised to place an Order		

Counter Eavesdropping

Definition of eavesdropping

1. Eavesdropping is defined as: The gathering of any information using audio, visual, cyber, or technical attack methods leading to loss or unauthorised disclosure of data or information **[Redacted]**

Organisation of counter eavesdropping within government

2. **[Redacted]**

3. The department "UK National Authority for Counter Eavesdropping (UKNACE)", which operates within the Foreign and Commonwealth Office Services Executive Agency, is the UK National Authority for counter eavesdropping (CE). It is responsible for **[Redacted]** providing CE advice and technical "sweeps" for all UK Departments, both in the UK and overseas. UKNACE can also supply a range of operational support, services and products. **[Redacted]**

It should be noted that there is currently no accreditation scheme for commercial CE Services or equipment and they are not permitted to work on Government property. Accredited training in the use of technical search equipment and techniques is, however, available to certain UK government and public service organisations. This can be arranged by contacting UKNACE.

The threat from eavesdropping

4. **[Redacted]**

5. To ensure "Confidentiality, Integrity and Availability" a counter eavesdropping risk assessment must be carried out and recommendations must be implemented when considering Physical, Personal and Information Security and Business Continuity arrangements. It has to be borne in mind that technological developments could mean that the eavesdropping threat will increase. In addition, information on eavesdropping attack methods are now readily available on the Internet.

6. Eavesdropping differs from many other threats to protectively marked information in that there is often no tangible evidence that information has been targeted. It is difficult to detect

an attack unless a physical eavesdropping device is found or confirmation is given by defectors or informants; even then it is difficult to conduct a thorough damage assessment unless specific discussions that might have been compromised can be identified. Given the difficulty in proving if an attack has taken place, there may be a tendency to suspect that an unexplained leak of sensitive information is the result of an eavesdropping attack.

7. The level of eavesdropping threat will not be the same for all departments and agencies and their List X contractors. For some organisations counter eavesdropping will not be a significant concern where the threat of eavesdropping is negligible. If the threat is higher then a risk assessment must be undertaken and any recommendations must be implemented.

8. The threat of eavesdropping relates primarily to protectively marked assets. The use of the term 'protectively marked' may seem inappropriate in the context of eavesdropping as, in the literal sense, the spoken word does not bear a protected marking in the same way as a document does. However, the target of the eavesdropper should be aware of the sensitivity of any spoken information **[Redacted]** and should know if such information would attract a protective marking should it appear in written form.

9. There may also be assets which do not in themselves warrant a protective marking but the compromise of which could damage the integrity and reputation of HMG or cause serious embarrassment. The counter eavesdropping threat can, therefore, extend to targets beyond the scope of the formal protective marking system.
In addition to protectively marked information, List X contractors are likely to have commercially sensitive information which would be attractive to competitors and consequently could be at risk from an eavesdropping attack.

10. It is likely that an attacker will be targeting information on a particular subject. But the nature of eavesdropping is such that he will almost certainly obtain information on other subjects too that he will also seek to exploit.

11. There is a wide range of commercial eavesdropping devices of increasing sophistication on the market. It is likely that such devices are being sold for use by private investigators engaged in domestic enquiries. Commercially sensitive information is more likely to be targeted than protectively marked material. It is important though, to put the threat from eavesdropping into perspective.

12. **[Redacted]**:

a) **[Redacted]**
b) **[Redacted]**
c) **[Redacted]**
d) **[Redacted]**
e) **[Redacted]**
f) **[Redacted]**
g) **[Redacted]**

13. The eavesdropping threat derives from:

a) the intelligence services of foreign powers

b) terrorist, extremist and subversive organisations

c) criminals, investigative journalists, investigation agencies, information brokers, companies seeking to acquire protectively marked information

d) Opportunist.

e) disgruntled employees who may have been suborned by any of the above.

14. **[Redacted]**.

15. **[Redacted]**

[Redacted]

16. **[Redacted]**

The law and eavesdropping

17. The law does not prohibit eavesdropping nor is it an offence to make, store, buy or sell an eavesdropping device. But installing an eavesdropping device may involve trespass, including in certain circumstances criminal trespass, and an offence of criminal damage. The transmission of eavesdropping product by wireless telegraphy may involve an offence under the ***Wireless Telegraphy Act 1949***, unless the transmission takes place under the authority of a licence issued by the Secretary of State or is exempted from the Act's licensing regime. Finally, the interception of communications in the course of their transmission on a public telecommunication system is an offence under the ***Regulation of Investigatory Powers Act 2000***, unless carried out under the authority of a warrant issued by the Secretary of State.

Methods of eavesdropping attacks

18. The list below provides an overview of the main methods of mounting an eavesdropping attack. **[Redacted]**

19. When considering eavesdropping methods of attack, it is important to differentiate between what is possible technically and what is feasible. An attacker will usually employ the simplest form of attack that provides results:

- **[Redacted]**
- **[Redacted]**

20. Most eavesdropping devices need a power source and a means of recovering the data, audio or visual information being targeted. The device can be powered by battery, mains electricity or cabling infrastructure, **[Redacted]**

[Redacted]

Application of counter eavesdropping within government

Baseline measures

21. Within sites, buildings or rooms used for the processing or storing of assets up to the same level of protective marking must have the appropriate physical, procedural and personnel security measures in place to protect such assets. For further details please refer to Mandatory Requirements 50, 51, 53, 54, 55, 57, 68 and 70.

In the UK, the implementation of appropriate physical and personnel security measures must be calculated using risk assessment methodology, if the treat is greater than negligible, to provide sufficient protection against an eavesdropping attack.

22. Visible building access controls are an effective deterrent to any potential eavesdropper. Good building design is also important. **[Redacted]**

Vulnerabilities

23. The risk of an eavesdropping attack can be assessed by considering the level of threat against the degree of vulnerability – refer to MR 5. As vulnerability relates specifically to the area in which sensitive discussions are held, only the organisation involved is able to make a

valid assessment of the risk.

Multi-occupancy buildings or those with party features are more vulnerable to eavesdropping attack than buildings in which a single organisation resides

24. **[Redacted]**

[Redacted]

[Redacted]

25. **[Redacted]**

[Redacted]

26. **[Redacted]**

[Redacted]

27. **[Redacted]**

[Redacted]

28. **[Redacted]**

29. **[Redacted]**

[Redacted]

30. **[Redacted]**

31. **[Redacted]**

    a) **[Redacted]**

    b) **[Redacted]**

    c) **[Redacted]**

    d) **[Redacted]**

    e) **[Redacted]**

32. **[Redacted]**

- **[Redacted]**
- **[Redacted]**
- **[Redacted]**

33. **[Redacted]**

a) **[Redacted]**

b) **[Redacted]**

c) **[Redacted]**

d) **Redacted]** .

e) **[Redacted]**

[Redacted]

34. **[Redacted]**

[Redacted]

35. **[Redacted]**

36. **[Redacted]**

[Redacted]

37. **[Redacted]**

[Redacted]

38. **[Redacted]**

Counter eavesdropping training

39. **[Redacted]**

40. UKNACE also offers Technical Surveillance Counter Measures (TSCM) training in a range of courses with optional accreditation by UKNACE. The training is available to certain UK government and public service organisations. **[Redacted]**

It should be noted that some commercial companies offer training in CE but none are officially approved.

Appendix 1

Request for advice on counter eavesdropping

To request advice it is desirable the following is completed before contacting the UK National Authority for Counter Eavesdropping (UKNACE).

[Redacted]

Department:

Location:

DSO/Contact Name: Tel No:

Description of Site: (For example, perimeter control, parking areas, include map if possible)

Description of Building: (For example, number of floors, access points, shared tenancy)

Religious Dress and Protective Security

Background

1. A person's religion or belief can influence the way they dress and present themselves in public. In most instances such clothing will present few, if any, issues in relation to protective security.

2. An example of religious items of clothing that may require some practical protective security consideration is the Niqab, or similar religious veils sometimes worn by Muslim women. Any item of religious dress that involves the full covering of the face will require organisations to consider how to balance the needs of religious and cultural observance with those of protective security, particularly in relation to access controls, photo passes and associated facial recognition requirements.

3. The following guidance is designed to assist Departmental Security Units in relation to the matters that should be borne in mind, including the legal considerations, although departments should seek specific legal advice from departmental legal advisers when formulating their own policies.

Access Controls, Photo Passes and Facial Recognition

4. The Security Policy Framework (SPF) recommends the use of photo passes to support access to sites, primarily to deter passes being lent to another individual or the finder of a lost pass using it to gain unauthorised access (See MR 56 for guidance). Whilst many access control systems themselves are automated (swipe card/barrier systems), the capacity to validate photo passes via facial recognition both at access control points and

within premises if security concerns arise offers an important layer of security and exercises a significant deterrent effect. A similar requirement to validate a photo credential via facial recognition exists for passport control at entry to the UK.

5. Essentially, any consideration concerning the removal of facial coverings should be functional; that is, on the basis that the facial covering prevents a person from seeing an individual's face. The primary consideration therefore for any security organisation is the degree to which not being able to see someone's face potentially compromises security. Depending upon local circumstances, a distinction can potentially be made between situations where it is essential (for example for purposes of validating access controls) or other situations where it may be desirable (for example within secure premises generally) for facial coverings to be removed.

The Legal Perspective

6. Any controls requiring individuals to remove a facial covering will involve treating a category of Muslim women differently to others and could, potentially, found a claim for discrimination under employment or equality legislation. Also relevant is the Human Rights Act 1998, and in particular Article 9 of the ECHR which enshrines the right to freedom of thought, conscience or religion, subject to certain limitations.

7. It would be for the department concerned to show that the controls were necessary and proportionate.

8. Generally, establishing an acceptable policy that is legally defensible is dependent upon demonstrating that the wearing of the niqab or similar veils in particular circumstances is detrimental to security arrangements, and that any policies are proportionate to assessed security risks and could not be achieved by another mechanism. A coherent approach is required within departments, although as with all security measures it may not be necessary to apply the same policy in all locations. Detailed legal advice should be sought from departmental lawyers in drawing up any such policy.

9. Any challenge to a policy requiring that facial coverings should not be worn, or should be removed at certain times, will need to be defended on the basis of the necessity for facial recognition checks in the particular circumstances of the department / location in question, and the proportionality of the controls in place. It will be necessary to show that a policy is in pursuit of a reasonable objective, reasonable, justifiable and proportionate.

10. Such justification is always going to need to be fact specific, and for that reason, it is not possible to provide detailed guidance on what will or will not be legally defensible. However, the following factors have been found by the courts to justify indirect discrimination in certain circumstances:

a. Flexibility on the part of those imposing the policy
b. The absence of other practicable measures
c. The cost of alternative measures, if combined with other factors
d. Security considerations, and in particular the ability of those imposing the policy in identifying the risks within their own premises, location etc.

Developing Local Policies and Practice

11. Whilst the instances of staff wanting to wear a veil or similar is not expected to be widespread departments are encouraged to develop local policies and practice so that if the issue does arise it can be addressed effectively and sensitively. These policies should reflect local risk assessments which may vary, and be documented and accessible to staff generally.

12. To arrive at an acceptable local policy in respect of the niqab, similar veils or other face coverings generally departments will want to consider what access controls are already in place and why. Where photo passes are required to access a site, departments will want

to apply this policy consistently and ensure any staff who wish to wear a religious veil can be photographed unveiled in circumstances where they feel comfortable (see below).

13. Departments will also want to consider what additional procedures may be necessary to ensure any photo pass issued to an individual who generally wears a veil can be verified as and when required. Such verification may be at the point of entry or subsequently within controlled premises if security concerns lead to individuals being challenged by staff for identification purposes.

14. Departments will want to think imaginatively as to whether alternative mechanisms could meet the security need: for example requiring individuals to confirm a password or pin entry. However where a risk assessment demonstrates a pressing security need to verify credentials via facial recognition departments will want to ask staff to remove the niqab.

Visitors

15. Departments will want to consider whether similar controls should apply to visitors. If they are to be escorted, or subject to other security measures, it may not be necessary to apply the same controls/conditions if the risks differ.

Other Security Related Circumstances

16. Departments will also want to consider other security related circumstances where it maybe necessary for a member of staff to be asked to remove a veil or similar facial covering. These could include vetting interviews where it maybe important for investigating officers to verify identity against photo id or be able to read facial signs or reactions to questions.

Implementation

17. It is important to appreciate from the outset that for Muslim women who do choose to wear the *niqab* or similar veils, it is an important element of their religious and cultural identity. Whilst there may be a diversity of opinions and debates between Muslims about the nature of dress required, the starting point should be respect for the choice made, and for each woman to decide on the extent and nature of the dress she adopts.

18. In those instances where face coverings need to be removed, this should be treated in a culturally sensitive fashion. It is strongly recommended that any relevant staff should have attended suitable briefings and diversity events so that they can appreciate the context in which individuals choose to wear religious dress such as the niqab and why it is important to them. Individuals have the right to request that only same gender staff be present when a covering is removed and this should be done in private. If a Muslim woman was available to perform the check this would be preferred, but if not a non-Muslim female officer could do so.

The Government Response Level System

Background

1. There are three Security Response Levels that apply to the Government Sector of the Critical National Infrastructure. This system also applies to some other sectors in the CNI.

1.1 The three Response Levels are:

- NORMAL
- HEIGHTENED
- EXCEPTIONAL

1.2 The three levels signify increasing security measures to be implemented in response to an increase in the assessed terrorist threat to government departments and related organisations.

1.3 Departments should calibrate their security arrangements to ensure a visible increase in security at each higher level of response. A range of BASELINE and INCREMENTAL security measures are required at each Response Level.

Response Levels

2. The appropriate Response Level for the Government Sector is set by the Cabinet Office. **[Redacted]** The table below illustrates the approximate relationship between the Terrorist Threat Levels and the Response Levels.

Threat Level	Response Level
LOW	NORMAL
MODERATE	
SUBSTANTIAL	HEIGHTENED
SEVERE	
CRITICAL	EXCEPTIONAL

2.1 The following non-protectively marked wording have been developed as a broad description to allow Ministers to be more open on the nature of the threat facing the UK from international terrorism and our approach to managing the associated risks.

NORMAL: Routine baseline protective security measures, appropriate to the business concerned.

HEIGHTENED: Additional and sustainable protective security measures, reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.

EXCEPTIONAL: Maximum protective security measures to meet specific threats and to minimise vulnerability and risk

2.2 **[Redacted]**

[Redacted]

Security Awareness

3. All staff in government departments should be familiar with Response Levels and the security measures that they should adopt. You will need to display the Response Level clearly (but beyond public foyers) within the staff entrances to your buildings. Any changes

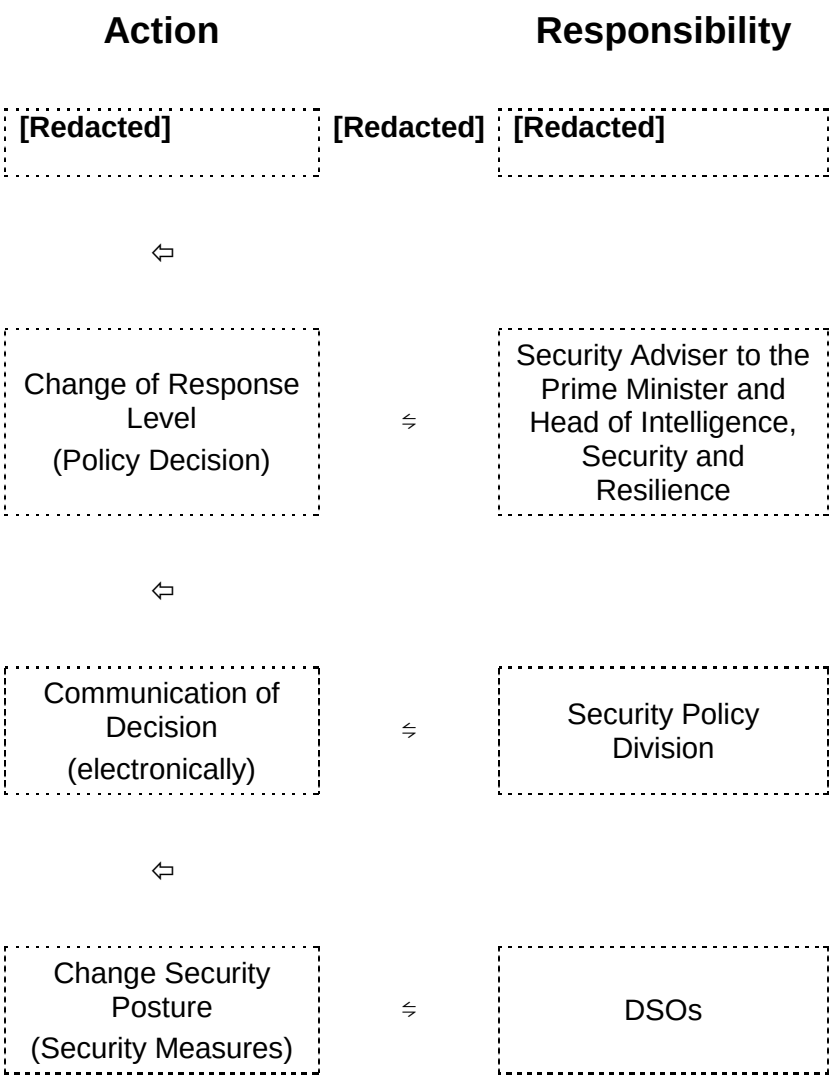
should be brought to people's attention immediately e.g. via an email or notice on your intranet. The national Terrorist Threat Level for the UK is made public **[Redacted]**

Response Level Changes

4. The Security Adviser to the Prime Minister and Head of Intelligence, Security and Resilience determines changes in the security response level for the Government Sector. **[Redacted]**

4.1 The decision to increase or decrease the response level is currently communicated to departments by the Cabinet Office Security Policy Division. **[Redacted]**. It is your responsibility to inform SPD of any changes to your contact details **[Redacted]**

The process is illustrated below:



4.2 DSOs should ensure that their department is prepared and update their security plans and policies to respond to a Response Level change immediately – both in and out of office hours. It is also DSO's responsibility to ensure that staff understand how to implement any additional security measures or plans.

Tests

5. To ensure that the Response Level system continues to function effectively and efficiently the system will be tested **[Redacted]**, either in or out of office hours. Currently, **[Redacted]** is sent to departments asking them to confirm receipt of the message, and that arrangements are in place to increase the Response Level and implement additional security measures. **[Redacted]**

5.1 Further information regarding the operation of the Response Level system can be obtained from Cabinet Office Security Policy Division, on **[Redacted]**, or e-mail **[Redacted]**.

[Redacted]

6. **[Redacted]**

6.1 **[Redacted]**:

- **[Redacted]**
- **[Redacted]**

[Redacted]

[Redacted]

7. **[Redacted]**:

- **[Redacted]**
- **[Redacted]**

[Redacted]

8. **[Redacted]**:

- **[Redacted]**
- **[Redacted]**

Procedural Measures

9. As well as ensuring that the appropriate Physical Measures are applied to their buildings Departments must also ensure that Procedural Measures are implemented at all their locations. These Procedural Measures must be put in place to deliver a number of security objectives to establish an appropriate level of security.

9.1 These Procedural Measures are grouped under five security headings:

- Communications and Staff Briefing
- Access Controls and Entry Checks
- Internal Measures
- External Measures
- Travel Security

9.2 Departments ***must*** address how they will meet the security objectives described beneath each of the security headings. Beneath each objective is a range of specific measures that must be implemented.

9.3 **[Redacted]**

Redacted]

Incremental Measures

10. Incremental Measures are those additional non-structural arrangements that should be put in place to deliver a number of security objectives to establish an appropriate level of counter-terrorist security policy at the increasing Response Level (NORMAL, HEIGHTENED, EXCEPTIONAL). Again these are grouped under five security headings:

- Communications and Staff Briefing - **[Redacted]**
- Access Controls and Entry Checks - **[Redacted]**
- Internal Measures - **[Redacted]**
- External Measures - **[Redacted]**
- Travel Security - **[Redacted]**

10.1 The Incremental Measures are intended to build upon the Baseline Procedural 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.

Departmental Plans

11. Departmental contingency plans (described in the Policy Framework section) should cover which Incremental Measures will be put in place at each increasing Response Level. When preparing their plans, Departments should always bear in mind that although these measures are graduated against particular Response Levels, this is for the purpose of general guidance and varying circumstances and local conditions may require the earlier adoption of measures advised at a higher Response Level. Departments will want to ensure their planned incremental action in the event of an increase in the Response Level, including all the necessary personnel, equipment and materials, can be implemented at short notice.

11.1 **[Redacted]**

Applying the Measures

12. **[Redacted]**

Security Posture

13. The list of measures is not exhaustive and Departments must consider what other steps are required or can be implemented at their locations to meet the counter-terrorist security objectives. When preparing plans Departments must bear in mind the overall objective of developing a security posture for buildings that visibly increases at the rising Response Levels. When preparing plans Departments should consider the definitions of the Response Levels described above and calibrate their security response accordingly.

Annex A - [Redacted]

Annex B - [Redacted]

Annex C - [Redacted]

Annex D - [Redacted]

Annex E - [Redacted]