Understanding the Security Policy Framework

What is the Security Policy Framework?

The Security Policy Framework (SPF) describes the standards, best practice guidelines and approaches that are required to protect UK Government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk managed approach to security that enables government business to function effectively, safely and securely.

What is Protective Security?

Protective Security is a risk management process to protect assets and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. The Government processes huge volumes of sensitive information (from personal data to matters of national security) and manages assets and services that are critical to public safety and the UK's way of life. It must guard against a range of threats including negligent behaviours, criminality, terrorism and espionage, as well as natural hazards such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security. Protective Security, particularly with regard to information security, is often expressed in terms of Confidentiality, Integrity and Availability - i.e. that security controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

Who is the SPF for?

The SPF is applicable to all Government Departments and Agencies and those bodies that are directly responsible to them. It should be extended, where necessary, to any organisations working on behalf of, or handling HMG assets, such as Non-Departmental Public Bodies (NDPBs), contractors, Emergency Services, devolved administrations, Local Authorities, or any regular suppliers of goods and / or services. Departments should consider where and what level of compliance is required of their delivery partners, and where equivalent security policies may be

acceptable based on risks judgements. Organisations wishing to adopt the framework should note that this website does not provide all the guidance necessary to implement effective protective security and they should contact Cabinet Office to obtain further information.

Why is the Government putting its security measures in the public domain?

The Government is committed to greater transparency as far as this can be achieved without introducing or increasing vulnerability. This also reinforces greater accountability across HM Government by committing Departments to publicly available security standards. The Government has a duty to lead in this process, however ultimately, security is the responsibility of everyone and it is important to increase public knowledge and awareness so that each one of us can play our part. Although much of the SPF has been made publicly available, it is necessary to restrict access to some technical and procedural material on security grounds.

Ho0w is the SPF structured?

There are four tiers, or levels, each representing a key element (of increasing detail) within the Government's protective security system. An overarching security statement makes clear that security not only supports business goals, but must proactively be considered a business enabler, making government work better, safer and more confidently. Next are a set of five core security principles, highlighting accountability at senior levels, collective responsibility of all staff and contractors, and the need to employ trustworthy people. At the third tier is a series of concise key policy documents (Security Policies), which clearly identify (in green boxed text), the minimum mandatory outcomes. These are minimum requirements and some Departments and Agencies will need to do more, appropriate to their particular circumstances and risk tolerance. The four policy areas are:

Security Policy No. 1: Governance and Security Approaches
Security Policy No. 2: Security of Information
Security Policy No. 3: Personnel Security
Security Policy No. 4: Physical Security and Counter-Terrorism

The tier four level contains an assortment of detailed technical standards, supplementary policy and best practice guidance. Much of this material is sensitive and can only be made available to those with a specific 'need to know'. However, where there is universally applicability, added value,

and no increase in vulnerability, material has been made publicly accessible at this level. Tier 4 provides the tools to support the core policy and principles; it will be updated regularly to ensure currency, address emerging vulnerabilities and adapt to the changing threat picture.

How is the SPF developed and approved?

The Government Security Secretariat (GSS) within the Cabinet Office is responsible for developing and maintaining the framework. The GSS work closely with a variety of security agencies and organisations across government. The main partners in developing the SPF are the Centre for Protection of the National Infrastructure (CPNI, http://www.cpni.gov.uk), the National Technical Authority for Information Assurance (known as CESG, http://www.cesg.gov.uk), and the Office for Cyber Security and Information Assurance (OCSIA) and Civil Contingencies Secretariat (CCS, http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx) within the Cabinet Office.

The SPF is endorsed by the Official Committee of Security (SO) which is chaired by the Cabinet Secretary and Head of the Civil Service, Sir Gus O'Donnell. It is updated on a regular basis with a refreshed edition every six months.

Any further queries should be directed to:

General enquiries
CabinetOffice
70 Whitehall
London SW1A 2AS

Switchboard: 020 7276 1234