Security Framework 1.0

Note from Jerry Fishenden: I have been unable to source the original PDF. This has been assembled from the HTML version sourced via the Wayback Machine / Internet Archive. It lacks the diagrams that would have been included.

Introduction and Scope

It is the aim of the Modernising Government programme to move towards the electronic delivery of government services. This document presents the framework for the expression of security requirements for such Information Age Government (IAG) services. The scope of this document includes functional security requirements appropriate for the delivery of services by, and on behalf of, government. It is applicable to those systems responsible for the delivery of services to citizens and businesses. These outward-facing systems may call upon services of internal departmental systems. It is assumed that such departmental systems meet the requirements of the Manual of Protective Security and are outside the scope of this framework.

These security requirements are also applicable to the delivery of government services by third party organisations. The security requirements expressed in this framework document represent a call for general alignment with best e-commerce practice, to which government believes it must itself conform.

This framework document and others derived from it are intended to be implementation-independent expressions of security requirements. Implementation constraints are limited to only those necessary to meet government security requirements. Suppliers are free to propose differing implementations constrained only by any interoperability requirements which may be necessary for operational reasons.

This framework document does not identify specific services as it is intended to apply to the provision of services in general. Annex A presents a set of example scenarios which illustrate many of the security issues to be addressed. This list is not intended to be complete and will be added to and amended as experience with electronic service provision develops.

This document currently addresses only functional security requirements and those functional aspects of the implementation that permit the services to be readily assured. Assurance will also be needed to ensure the presence and proper operation of those functions. There are currently a number of initiatives and processes for attaining assured implementations. However, assurance requirements for Information Age Government are subject to further discussion.

Purpose of this Document

This document sets out a framework for the expression of security requirements for the procurement and acceptance of IAG services and their implementation. As such, it is of interest to organisations seeking to establish such services and suppliers who wish to offer services themselves or equipment to support IAG services.

It is also relevant to security authorities who may use this document to assess the suitability of offered solutions and accredit them for operational use.

Document model for IAG security requirements definition
This framework document is a high level expression of requirements and expands upon the security statements in the e-government strategy ["e-citizen e-business e-government"]. Other related and more detailed requirements statements will address specific topic areas. Figure 1 below depicts the document relationships.

[NOT AVAILABLE] Figure 1 — Security Framework Documents RTF

This high level security framework will be supported by more detailed requirements statements for the specific topic areas below:

a. The IAG Authentication Framework covers the security services required to ensure that users are uniquely and unambiguously identified and granted access only within the authorisations made. All systems security ultimately rests upon the capability to identify and appropriately authenticate system managers and users possessing privileges in respect of the system assets.
b. The IAG Trust Services Framework covers the security services required to ensure that transactions are properly traceable and accountable to authenticated individuals and cannot subsequently be disavowed.
c. The IAG Confidentiality and Privacy Framework covers the security services required to ensure that information is stored and transferred securely.
d. The Business Services Security Framework covers the security services required to ensure that the IAG service applications themselves are designed, configured, and operated in a secure manner and their information assets properly protected. The business applications include the web servers that present the service to the users and the back-office systems that host the applications services themselves. The first draft covers the web server hosted services only.
e. Network Defence Security Requirements covers the security services required to ensure that the plant, stored data, and other assets of the IAG service are properly protected against malicious attack and non malicious failures.

The vehicle for requirements expression is based upon the Protection Profile concept developed for the international security evaluation criteria (Common Criteria). Annex C summarises the Protection Profile concept.

The requirements expressed in this framework represent a baseline for discussions and agreements as to what constitute adequate and acceptable security measures. It is recognised that, subject to a risk assessment, not all requirements may be applicable in all cases, and that in some cases it may be technically or economically infeasible to meet the requirements fully.

When using these requirements as a basis for assessing the acceptability of a potential service offering, the aim should be to meet those requirements that are applicable to the

specific service. Where a requirement is not met the reasons for this must be presented and agreed with the IAG service authorities as acceptable.

The agreed requirements will then be used as input to the design and implementation of the service and in the subsequent accreditation for operation. This process is depicted in figure 2 below:

[NOT AVAILABLE] Figure 2 — Application of Framework RTF

Service Security Environment
Environmental Assumptions 14 To meet the objectives of IAG, it is assumed that the delivery of government services will share the same public network infrastructure that is being used in the community at large. In particular, the Internet will be a principal means by which public access to government and government services will be achieved though others such as interactive digital television and call centres will be used. The security domain model is illustrated in figure 3 below.

[NOT AVAILABLE] Figure 3 - Security Domains

The Public Network Domain (PND) contains that part of the communications infrastructure that lies outside the control of IAG operators and clients. In the case of Internet delivery, it must be assumed to be accessible to potential threat agents and provide a transmission capability with no service quality commitments. In the IAG context, the PND includes the Internet and service providers that provide the Internet access and may also include the PSTN, interactive TV, and other communications platforms.

The IAG Service Provision Domain (IAGSPD) contains that part of the communications infrastructure, which is under service providers' control and used to host the services. The early IAG proposals view the IAGSPD as a government Intranet as typified by the GSI. Where services are jointly provided by different, possibly non-government, organisations, the IAGSPD security requirements will apply across the heterogeneous network infrastructure supporting the services. It is a requirement that the IAGSPD be adequately protected against outside attack in accordance with applicable policy.

A Departmental Service Provision Domain (DSPD) contains IT infrastructure used to host all or part of a government service and is under the management control of the department offering the service. The DPSD is assumed to lie wholly within the IAGSPD that is used to communicate between different DPSD regions. For this reason it is preferable that all IAG departments subscribe to, and use, the GSI for direct provision of IAG services.

A Non-Departmental Service Provision Domain (NDSPD) contains IT infrastructure used to host all or part of an IAG service supported by a non departmental body and is under the management control of the organisation offering or contributing to an IAG service. The NDSPD is assumed to lie wholly within the IAGSPD that is used to communicate between the distributed service elements. It is preferable that a NDSPD be accommodated within the GSI or its affiliated secure networks. If this is not the case, service providers will have to demonstrate that the security requirements have been satisfied external to the GSI.

A Client Network Domain (CND) is that element of the IT infrastructure under management control of the client which is used to support access to the government services. The CND may be a single domestic PC connected via an ISP to the IAGSPD, in this case the ISP lies within the PND. Alternatively, the CND may be a complete corporate Intranet comprising many workstations under a more formal control. The practical level of trust in the CND will depend on the extent of the management controls exercised but, as it lies outside the IAGSPD, no assumptions of trust can be made about the CND environment.

The Client Side Service Domain (CSSD) is that element of the CND that is supplied by or on behalf of IAG services and installed within the CND to encapsulate important trusted elements. IAG service management will exercise some control over the content of (but not necessarily the delivery of) the CSSD. The goal is to deliver the CSSD functions embedded in a trusted Smart Card or similar token though initial deployments may not achieve or require this.

The Trusted Service Provider Domain (TSPD) is that element of the IAG service infrastructure that is operated under a service agreement on behalf of government by a commercial service provider. The TSPD is operating as an agent of government and is expected to meet the standards necessary to act as a government agent or proxy. In general, security requirements levied on the IAGSPD are applicable to the TSPD and will form part of the conditions of operation. The TSPD will typically be connected only to the PND but will have a privileged relationship with the IAG service providers.

Figure 4 below illustrates how these security domains map on to one envisaged implementation approach for government service delivery via the GSI and Internet to a user's domestic PC.

[NOT AVAILABLE] Figure 4 - Example IAG Service Delivery Model

External Security Policy Framework

The implementation of IAG networks and access must take place within the legislation that applies to the handling of national/international, commercial, and personal information within public and corporate networks and information servers.

The individual government departments and service agencies will also possess their own corporate information handling and security policies which provide more detailed interpretations of the national or corporate policy and legislative frameworks and address the business continuity requirements of the organisation. Organisational policies are not cited explicitly but are assumed to express requirements for good business practice. In addition, government aims to take a lead in the setting of and conforming to high standards of management in its control of publicly owned assets and information.

The following are the principal pieces of legislation and proposed bills that inform the security requirements for IAG implementations

a. The Human Rights Act and the underlying European Convention on Human Rights set out everyone's right to privacy in their correspondence.
b. The Data Protection Act sets requirements for the proper handling and protection of personal information held within information processing systems.
c. The forthcoming Electronic Communications Bill sets the requirements for electronic signatures and their equivalence to conventional signatures.
d. The Interception of Communications Act makes it an offence to intercept communications on a public telecommunication system. Case and time limited exemptions may be granted subject to warrant.
e. The forthcoming Regulation of Investigatory Powers Bill would maintain the offence of interception and extend it to private networks; it will also make regulations limiting access by employers to communications used by their employees.
f. The Wireless Telegraphy Act controls the monitoring of wireless telegraphy.
g. The Police And Criminal Evidence Act defines conditions under which law enforcement may obtain and use evidence.
h. The Computer Misuse Act makes attempted or actual penetration or subversion of computer systems a criminal act.
i. The Public Records Act lays down requirements for the proper care and preservation of documentary records of government activities.
j. The Official Secrets Act lays down requirements for the proper control of government information.
k. The Freedom of Information Bill would lay down the citizen's rights of access to government held information.

Extant Security Standards

BS7799 [Ref BS7799-1/2:1999] presents a code of practice (Part 1) and requirements specifications (Part 2) for establishing, implementing, and documenting the security of information management systems. It provides a set of controls which, when implemented, will ensure best practices for IAG services in specific installations are met.

The UKAS approved c:cure scheme tests for full compliance through external audit and awards accredited certification for full compliance. It is government policy to move to BS7799 compliance. For government purposes, either c:cure or internal accreditation may be acceptable.

Part of BS7799 compliance is a full risk assessment. The government preferred method is a CRAMM review and an HMG Infosec Standard 1 analysis.

The Manual of Protective Security contains general requirements and guidance for the handling of protectively marked information, both in electronic and other forms. It is the reference document for information marked RESTRICTED and above and should be used when interpreting these requirements for protectively marked information. It provides the government guidance for the implementation of BS7799 controls.

ITSEC and the Common Criteria for IT Security Evaluation provide a set of functional classes and assurance criteria upon which a formal evaluation and certification process can be

based. The extent to which formal evaluation is applicable to IAG services has yet to be established.

TScheme is the co-regulation scheme for encryption service providers in the UK and is developing a set of profiles and an assessment scheme to demonstrate profile conformance. It is proposed that IAG services will make use of external Trust Service Provision and may therefore wish to call up the tScheme profiles as part of an IAG trust service provision agreement.

Threats to IAG Services

In considering the protective measures that should be put in place within IAG systems, a risk analysis must be performed. This risk analysis must consider the intent, motivation and capability of sources of threat, the feasibility of methods of attack, the nature of vulnerabilities that may be exploited, the value of assets to be protected, the consequences of a successful attack, and the costs of any countermeasures.

Threat analysis examines the assets that require protection, the potential sources of threat, and the likely methods of attack. Annex B describes some threat scenarios that are relevant to IAG services.

IAG Service Assets

The following are assets of IAG based services which require protection:

a. The Personal Data relating to a client for any IAG services must be protected against loss, damage, or unwarranted disclosure in line with the relevant data protection and privacy legislation. It is important to note that personal data, once transferred to the CND from the IAG service, is outside the scope of the IAG service, which can take no responsibility for it. Users are responsible themselves for the proper protection of their personal details when they are under their personal control.

b. The Corporate Information Base of government in general and organisations offering IAG services must be protected against loss, unwarranted disclosure, or introduction of erroneous content.

c. The IAG Service (comprising the applications and delivery platforms) must be protected against threats to its availability and integrity of the service offered.

d. Authentication Credentials must be protected against forgery or unwarranted use.

e. Objects that represent monetary or other Value must be protected against fraud. Some of the IAG transactions are likely to result in cashable orders which must be properly controlled, some may relate to the delivery of goods that can be misappropriated.

Potential Sources of Threat

An authoritative statement on the level of threat that potential threat agents pose will be required on a regular basis in order to ensure that adequate countermeasures are in place. Such statements can be obtained from the Security Service who collate and assess threat information from their own sources and from other organisations involved in countering threats.

Inside Sources of Threat

Some of the potential threat agents are insiders for whom system authorities have some responsibilities and can exercise some control. These include:

a. Legitimate Users of IAG services may seek to misuse or damage the IAG service provision. Such individuals may possess, or have access to, significant technical resources and skills with a strong motivation to subvert the service — frequently for financial gain. Hostile users will have full access to their own CND from which to attack the service. Legitimate users of the service are likely to be subject to legal restraint if subversive activity is traced to them.

Legitimate users of IAG services may unintentionally damage IAG services. This is most likely to arise as a result of genuine mistake or poor user training. Such individuals are not generally motivated to undermine the IAG service provision but may nevertheless cause significant disruption

b. IAG Service Operators who are, or have been, responsible for the provision or operation of IAG services may seek to exploit that privileged position. This will generally include government employees or their agents (for example the TSPD) or employees of outside organisations contributing to IAG services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation is likely to be fraud or personal dissatisfaction. Service operators and government employees are readily subject to sanction in the event that security breaches are traceable to them.

c. Insiders who are not associated with the provision of IAG services but who may share access to the IAGSPD. This will generally include government employees or their agents who have access to the IAGSPD but no responsibility for IAG service provision. These are individuals who are able to mount an attack from within the IAGSPD or TSPD and may possess a strong motivation to do so. Members of the IAGSPD will be readily subject to sanction; similar sanctions must be available for application within the TSPD.

External Sources of Threat

Some of the potential threat agents are outsiders and are beyond the control of the system authorities. These include:

a. Hostile Outsiders are individuals or groups who possess access to the PND but no other association with the IAG services. Such individuals may possess significant technical skills with a strong motivation to subvert the IAG service provision, either for personal gain or other reasons. They may reside outside the government jurisdiction and not be subject to sanction or cessation orders.

b. Criminal Organisations including organised crime groups as well as petty criminals may be attracted by the potential for large-scale fraud presented by IAG. Some IT related fraud is already known to have taken place.

c. Foreign Intelligence Services may seek to exploit IAG services as a means of obtaining information on the workings of government or on individuals of interest. There may also be a threat of attacks designed to disrupt the workings of IAG

although such attacks are only thought to be likely in times of heightened international tension.
d. Commercial Organisations may seek to acquire information about competing companies, customers, debtors etc from IAG related sources.
e. Investigation Agencies may seek to exploit IAG systems as a source of information on targets of interest — for example addresses or other personal details.
f. Terrorist Organisations may seek to exploit IAG systems as a source of targeting information on individuals. In the future, there may be a threat of electronic attack designed to disrupt or bring down IAG services.

Possible Methods of Attack
This section identifies the principal means by which the identified sources of threat may seek to attack IAG services and systems. As with the sources of attack, regular updates of the current state to the threat arising from the application of such methods will be required from the Security Service to ensure that the protective measures remain appropriate.

Electronic Attack
This section lists methods of attack that seek to exploit directly technical features and properties of the IT systems and plant that support the IAG services.

a. Hacking includes all attempts at unauthorised access to IT systems whether by insiders or from external sources. Methods include the exploitation of weaknesses in configuration or implementation, unauthorised use of access credentials, and internal breaches of operating procedures.
b. Malicious Software (including viruses) threaten the availability and integrity of IT systems. Specifically targeted introduced software may also threaten the privacy and confidentiality of stored information. The number of computer viruses in existence continues to rise. The sophistication and potential for damage possessed by modern viruses is significant. Most viruses are now passed as attachments to Emails but the risks posed by uncontrolled use of storage media should not be discounted.
Denial of Service flooding attacks are designed to render a target system temporarily unusable by overloading the external access points to the system with excessive numbers of requests for service.

Other Attack Approaches
This section lists those methods of attack that exploit indirectly the features of the IT systems supporting IAG services. There are many attack approaches that involve the behaviour of system users and operators.

a. Insiders are well placed to circumvent security installations designed to prevent attack from outside. Use of an insider is the preferred method of attack for many hostile organisations.
b. Deception may be practised by sophisticated attackers who may attempt to pass themselves off as users in order to achieve access to information of interest. This is already practised widely in telephone transactions and the potential exists for similar attacks to be carried out by electronic means.

c. Denial may be practised by attackers who may attempt to deny a commitment or obligation entered into as part of an IAG service action. If a legitimate transaction can subsequently be disavowed or otherwise challenged, opportunities for fraud are created.
d. Forgery may be used to create or obtain false access credentials and thereby gain unauthorised access to IAG services.
e. Theft may be used to obtain unauthorised control of legitimate access credentials, which may then be presented to gain unauthorised access to IAG services.

Accidental Damage

IAG systems need to be protected against threats of accidental damage. Because occurrence of such incidents is, by their nature, difficult to predict, it is impossible to obtain a precise assessment of the impact of such threats. Protective measures should be in place to guard against the impact of such eventualities where justified by their likelihood and the potential damage. Some possible threats to be considered are listed below.

a. Inexpert Users may unintentionally damage the IAG service provision. Whilst such user errors are unlikely to be motivated by an intention to undermine IAG services, they may cause significant disruption or damage by, for example;
unauthorised disclosure of information, for example personal information that could lead to fraud or undermine confidence in the system; failure to revoke user or manager rights once they are no longer required; loss of business information if, for example, access credentials are lost or the information is accidentally deleted.
b. Operators and administrators of IAG systems may also, through incompetence or inadequate training, cause damage to the service assets or its continuing availability. Such individuals are not specifically motivated to undermine the systems but, owing to the privileged positions they hold, may unwittingly cause significant damage
c. Equipment or software failure may lead to suspension of the service or damage to the stored information base;
d. Accident or other Disaster may destroy the service provision or the stored information base.

Security Objectives

The security objectives statements distil the threat, assets, and environmental assumptions into a set of control objectives which, if they are all met, ensure that the threats identified are properly countered in the declared environment. The principal environmental assumptions that relate to the provision of IT services are tabulated below.

Environmental Assumption Notes

1 — Open Delivery

IAG services are delivered using a public infrastructure over which the service authorities have little or no control. The requirement that no government special infrastructure is necessary to deliver the services, the Internet is seen as the delivery mechanism of choice though direct dial in over the PSTN may be acceptable in special cases. No assumptions can be made about the assurance in the client workstation.

2 — Existing Secure Networks
The systems hosting IAG services are installed and managed in accordance with existing policy and practice for government systems connected to other networks. A statement about the environment which cross references to existing codes of practice and policy on government and other service supplier data networks.

3 — Government Best Practice
IAG services must be implemented so as to conform to commonly understood 'best practice' and support the standards of probity that are expected of government actions. General statement that government typically sets standards for its own integrity and probity which do not lay it open to challenge.

4 — Unassured Client Domain
IAG services must be implemented in a way that permits adequate trust relationships to be established between the participants without requiring strong controls or constraints on the terminals used to access the services. The equipment used by members of the public to access the services are uncontrolled and typically under non technical management control that is unaware of security risks (eg a domestic PC). Government cannot place constraints on the state of such equipment as a condition for IAG service access. Security approaches will have to allow for this.

The objectives are necessarily high level and seek to minimise constraints on candidate implementations. Some of the objectives will be levied on the environment and trace to security requirements that the environment must be shown to meet. The security objectives are those for the IAG services themselves though not all are necessarily relevant to all services. The principal control objectives are tabulated below (cross-reference to BS7799 controls marked {BX x.y.z}. For BS7799 compliance, controls should be defined in terms of Part II Sections 4.1 to 4.10.

Service Control Objective Notes

OS1 — Effective User Identification & Authentication
Accountable IAG services are accessible only to those individuals and systems that have been authorised to access such services. {BS: 4.7.2} Will map on to a requirement for technical measures to ensure that access can only be obtained on presentation of properly constructed access credentials. Access is qualified as ‘accountable’ so as not to exclude some anonymous access (eg information only access).

OS2 — Effective User Registration
Access permission is granted only to those whose bona fides have been properly established. {BS: 4.7.2} Will map on to a combination of technical and procedural measures to ensure that users are properly identified and authenticated before being granted access — a significant problem in public access systems — and that false or multiple identities cannot be created.

OS3 — Effective Access Control

Access granted to IAG service applications and assets is the minimum necessary for the identified user to obtain the services required. {BS: 4.7.4} Will map on to a requirement to ensure that a user/administrator, once identified and authenticated, can access only those parts of the system and assets necessary to perform the authorised task.

OS4 — Effective User Access Management
Service authorities exercise complete control over the access rights granted to IAG service users. {BS: 4.8.3} Will map to the requirement to install and remove user profiles as required — without the involvement of the user. Technically will map to requirements for access revocation and, for example, certificate revocation schemes.

OS5 — Non Repudiation
Transactions are demonstrably traceable to the originator. {BS: 4.8.3} Service authorities must be confident that transactions enacted in the name of an authorised subscriber can only have been carried out by that subscriber. This frustrates attempted denial of responsibility for fraudulent use.

OS6 — Evidence of Receipt
Transactions are demonstrably traceable to the recipient. Users of the services must be able to demonstrate that transactions submitted have actually completed and that they cannot be falsely accused of failure to submit required returns or deny receipt of information.

OS7 — Trusted Commitment Service
Any commitments made using IAG services are not liable to theft or fraud. Authorised users of IAG services must be confident that (for example) their authorities for payment will be properly controlled and that they are not vulnerable to fraudulent use of their means of payment.

OS8 — Privacy and Confidentiality
Personal and other information submitted to services is not disclosed or visible beyond those authorised and with a need to receive it. {BS: 4.8.3} Personal details submitted by a client of IAG services must be properly protected at all times within the IAG service. Internally, within the service departments, information must be handled responsibly and securely.

OS9 — Integrity
Information received from or passed via the services is not altered or otherwise subverted. {BS: 4.8.3} Users of IAG services must be confident in the correctness, completeness, and authority of information and advice received in an IAG service transaction and that anything they submit will be correctly received.

OS10 — Service Availability
Continuing access to the service as and when required must be assured. {BS: 4.9.1} Users of the IAG service must be able to depend on the continuing availability of the service to meet their obligations with respect to government service provision — subject to limits imposed by the availability of the PND.

OS11 — Information Availability
Continued access to the IAG data assets as and when required must be assured.
{BS: 4.9.1} Data assets of the IAG service are an important record and must not be lost through accidental, careless or deliberate acts of IAG service users, administrative staff, or in the event of equipment failure.

OS12 — Service Protection
The IAG service implementation and associated assets must be protected against outside interference and penetration.
{BS: 4.2.2} The IAG services must be adequately protected from outside attack mounted against the service applications themselves or the underlying network infrastructure.

OS13 - Effective Audit and Accounting
The IAG service must keep a proper record of significant transactions. {BS: 4.10.3} A general requirement for a proper record of significant events which may have to be revisited. Required partly to meet external audit requirements, and partly as a mechanism for making users accountable.

Service functional security requirements
The service control objectives may be met by ensuring that the following functional security requirements are met by any proposed installation. These security requirements are, as far as possible, independent of specific techniques and technologies used to satisfy the requirements. However, the need to provide a universal service requires that some technical choices be made at the requirements level in order to secure interoperability.

For convenience, the security requirements are categorised by the primary security objective of the requirement, additional rationale provides greater detail on these relationships in order to demonstrate completeness.

OS1 — Effective User Identification and Authentication
User access to accountable IAG government services shall be granted to authorised users and system administrators only. The standard I & A requirement to limit access only to those who have been properly identified and authenticated.

User access privileges granted to IAG services shall be the minimum necessary to satisfy the business requirement for that service or management function. A standard privilege minimisation requirement to limit the potential for damage caused by authorised users and system administrators.

It is desirable that user access to accountable IAG services shall be conditional upon the presentation of an access token issued by or on behalf of government service providers. Access control can be made stronger through the use of properly designed access tokens. There is a strong preference for these to be used though there may be circumstances where the risks are low enough for tokens to be unnecessary.

User access to IAG services shall require the presentation of authentication credentials to identify the individual requesting access. An implementation requirement for personal

authentication beyond possession of the token. The type of personal authentication is not specified but will probably be a password unless biometrics is permitted.

OS2 — Effective User Registration
Access rights to IAG services shall be granted only when IAG service management or their agents are satisfied that the user is actually who he/she claims to be, is not already registered under a different identity, and has a legitimate need for access. A requirement to prevent impersonation or the issue of access rights to bogus individuals or the creation of multiple identities that could be misused. An individual may possess multiple roles with respect to IAG services but can only ever possess a single identity.

The actual means to achieve this can be decided later, as a minimum some evidence of existence (birth certificate?), identity (passport, driving licence?), and presence (signature?) is required if the transactions are significant.

For less binding relationships, less trust in the registration process may be sufficient.

OS3 — Effective Access Control
User access shall be possible only to those IAG system assets and services which are necessary to support the specific service requested. A requirement to enforce internal access controls at the object or application level such that a legitimate user, once granted system access, cannot influence or damage system data which the required service does not need.

OS4 — Effective User Access Management
The possession and issue of user access rights shall at all times be under the control of system management. General requirement for a management framework for user access rights.

It shall be possible for system management to revoke a user/administrator's access rights in a timely fashion without the presence or involvement of the user/administrator involved. Specific requirement to be able to revoke a users rights and without reference to him/her. Any access credentials and or tokens cease to have any validity.

It is recognised that immediacy may not be feasible, the aim should be for the revocation to take place as soon as possible bearing in mind the risks of misuse in the intervening period.

OS5 — Non Repudiation
The IAG service shall provide evidence that a transaction received from a user did actually originate from that user who cannot subsequently deny responsibility for the transaction. Requirement to provide a binding between transactions purporting to come from a user and actions of that user in person. The system should have some means of preventing a user subsequently denying responsibility for a transaction, or third parties falsifying a transaction that purports to come from a user.

The IAG service shall provide evidence as to whether a transaction received or claimed to have been received by a user did actually originate from the IAG service. Requirement to

provide a binding between transactions received from an IAG system and the actions of the system. The system should have some means of verifying the authenticity of information from the system and prevent users disputing the authenticity of information received, or claimed to have been received.

The IAG service shall provide evidence that information received from a user was actually submitted by that user and the service cannot dispute the authenticity of the information. Requirement to provide a binding between transactions from a user and the receipt of that information into the service. The user wished to be assured that he can prevent the IAG service disputing the authenticity of information received.

OS6 — Evidence of Receipt
The IAG service shall provide evidence that a transaction received from a user was accepted by the service and receipt cannot subsequently be denied by the service. Requirement to provide a strong receipting mechanism to users such that, in the event of a dispute, users are able to make a strong case that they have met their obligations with respect to the service provision.

The IAG service shall provide evidence as to whether a transaction dispatched to a user was actually received by that user and receipt cannot be denied by the user. Requirement to provide a strong receipting mechanism to the system such that, in the event of a dispute, system management is able to make a strong case that information apparently received by a user was actually received. The system should have some means of preventing a user falsely denying receipt of information or notice of required action.

OS7 — Trusted Commitment Service
The IAG service shall protect instruments of commitment from fraudulent use or other exploitation. Requirement to provide assurance that exploitable user payment authorities (such as credit card information) or other commitment vehicles are properly protected by the service. There may be a need to demonstrate this protection in the event of a dispute.
The IAG service shall provide auditable receipts for all commitments made with or via the service. Requirement to provide proper evidence of commitments made and received such that, in the event of a dispute, it is possible to demonstrate, for example, a payment history to an external auditor.

OS8 — Privacy and Confidentiality
The IAG service shall provide adequate protection of personal and private information from observation or disclosure when in transit across vulnerable network segments. A requirement to review the need for communications confidentiality. This is as required to meet obligations under privacy and data protection legislation. The measures should be appropriate for the threat and seek to deny access to all those not authorised.
In accordance with the Data Protection Act, the IAG service shall protect personal and private information from misuse when stored and processed within the IAG service implementation domain. A requirement to meet privacy and data protection obligations within the IAGSPD. This will require the service operators to demonstrate best practice and fulfil their legal obligations with respect to personal data. Note that personal information that is stored within the client domain is a client responsibility.

OS9 — Integrity

The IAG service shall protect information transmitted across public networks from exploitation by accidental or deliberate modification, deletion, or replay. A requirement for strong communications integrity measures to prevent an attacker from manipulating the data in transit or from loss and corruption caused by equipment or communications failures.

The IAG service shall protect service information stored within the unassured client domain from exploitation by accidental or deliberate modification. A requirement for storage integrity measures in the client workstation. This will prevent the user or other attacker from manipulating the stored context on the workstation in order to gain some advantage. A requirement to protect against unintended corruption will be met if deliberate corruption is controlled. Note that this is not intended to reduce the ability for a user to amend personal details stored locally. It relates to application data that is stored locally but is under service ownership — for example stored context between application sessions.

The IAG service shall protect information stored within the IAG service implementation from deliberate modification or destruction by outside attackers. A requirement for strong measures to frustrate 'hacking' attacks on the service which might undermine confidence in the service by maliciously altering user data or publicly posted information (eg modifying web pages).

The IAG service shall protect information stored or transferred within the IAG service implementation domain from accidental loss or corruption. A requirement for 'best practice' integrity measures within the service. Electronic signature based measures can be used where possible but it is probably adequate (and more readily implemented) to rely on standard access control techniques. This will also lead to a requirement to implement proper backup measures.

OS10 — Service Availability

The IAG service shall be protected against outside attack which seeks to damage or deny provision of the service to authorised users. A requirement for strong security measures to prevent the service being susceptible to external denial of service attacks.

The IAG service shall be protected against internal equipment failure which might damage or prevent continuing provision of the service. A requirement for best practice design approaches to prevent the service being unduly susceptible to failure following equipment failure. Will require a measure of redundancy consistent with the importance of continued service provision and the ability to effect swift repairs.

The IAG service shall be protected against loss of data, loss of equipment, and other external adverse events. A requirement for a business continuity plan and supporting measures. There is a general requirement to anticipate disasters and make sure that the necessary measures are instituted to avert disaster where possible and recover where prevention is not an option.

OS11 — Information Availability
The IAG service shall make provision for the retrieval of critical or personal data that has been damaged or destroyed by malicious or other actions. This is a business continuity requirement for a proper backup regime to ensure that the active datasets are secured and can be restored in the event of failure.

The IAG service shall make provision for retrieval of protected information in the event that a user or system administrator is unable to supply the necessary access credentials. This is thus a business continuity requirement to provide facilities to recover user data in the event that an access token or password is lost. This facility may also be required to support investigations of possible system misuse where the suspects might be alerted by requesting their credentials.

OS12 — Service Protection
The IAG service application and underlying network infrastructure shall be protected against outside attack that seeks to undermine continued service provision. Any system that is connected to public networks is open to attack by those seeking to damage or deface the service without necessarily seeking personal gain. The underlying networks must be hardened against such attack using measures such as boundary control and scanning devices. The applications themselves must be constructed in such a way that vulnerability to outside attack is reduced to an acceptable level.

OS13 — Effective Audit and Accounting
The IAG service application shall maintain a record of transactions that may require after the event analysis. General requirement for maintenance of audit and accounting logs. Reasons for requiring this include establishing accountability for transactions, reconstructing failed transactions, and furnishing evidence in the event of a dispute about services.

ANNEXES

Annex A
Example IAG Service Scenarios
This annex presents some representative scenarios to which the government service delivery security requirements might be applicable. The list is not intended to be exhaustive and is presented for discussion. These are examples only and do to imply any intent or commitment to offer such a service, nor are the analyses of the scenarios intended to be complete.

Scenario 1 — Single Department Transaction
A member of the public or a business wishes to carry out a service transaction with a single government department. The service has monetary and/or utility value. He/she accesses the ‘service entry page' for the service on the Web. He/she completes an electronic form, signs it as proof of identity and attaches any other certificates or documents necessary and submits the form. If appropriate, he/she authorises payment of the fee. The department actions the form and confirms with a dated and signed receipt either along with, or to be followed by, the deliverables of the service in question.

Examples include application for benefit, grant, licence, certificate of approval, registration of status or search of registration information, passport issue, tax assessment and coding,

Scenario 2 — Multiple Department Transaction
As scenario 1 but the transaction involves more than one department. In this case, the transaction requires action by multiple departments and the co-ordination of responses.

Examples include arranging long-term domiciliary care for the individual and business transactions such as arranging development grants, export credit guarantees, company registration details and returns, and VAT/PAYE/National Insurance.

Scenario 3 — Private Correspondence with Government
A professional (consulting engineer, barrister, etc) wishes to correspond with an official in a government department, via electronic media with a guarantee of confidentiality at least as good as conventional methods of communication.

Examples include members of the bar corresponding with the CPS on briefs, and consultants or suppliers acting on procurements.

Scenario 4 — Change of Personal Status
A member of the public changes some personal details. He/she is able to access a service which will capture the details of the change (when bona fides have been established) and communicate it to interested government departments. Confirmations are made available to the client.

Examples include change of name, home address, e-mail address, phone number, marital status, and death.

Scenario 5 — Employment Application
A job seeker browses vacancies using one of many electronic transmission media (Web, kiosk, interactive television, e-mail subscription list). He/she applies and (when he/she has provided proof of his/her identity) his/her CV is automatically called up if he/she has one stored. He/she has the opportunity to add modify or delete details.

If there wasn't a CV stored, he/she is invited to create one. He/she lists referees and contacts them to make sure they are happy to speak for him/her. He/she calls up certified qualification details by submitting a request to the relevant academic institution(s). Then he/she approves the application to be forwarded to the prospective employer. He gets a receipt from the employer either with or to be followed by notification of the results of the application.

Scenario 6 — Information Search
A member of the public browses public information provided by government and possibly enters into some commitment on the basis of the information obtained.

Examples include Foreign Office travel information (leading to some travel commitment), DTI business information (possibly leading to some contractual commitment).

Scenario 7 — Purchase of Government Information
A member of the public or a business queries a department for specific information. The client provides contact information and pays a fee if appropriate.

Examples include purchasing documents or information relating to policy formulation, historical information, or legal obligations.

Scenario 8 — Electronic Voting
A member of the public registers their intention to vote electronically in an election. They prove their bona-fides and this is checked against the voter's list and they are given an electronic ballot paper for the constituency in question. Between the time the electronic ballot box opens and closes they choose their chosen candidate and submit their vote. When the ballot closes, votes are scrutinised and counted, and the electronic count conveyed to the returning officer, for consolidation with the manual count.

Scenario 9 — Interdepartmental Request
A member of a Government Department service team has to deal with a query related to an application made via a 'Portal form' for a 'joined-up' service. They are logged in on their computer terminal so they can call up relevant data from other departments, agencies and local Government who are involved in the case as notified on the original submission. The details are checked and contact is made with other case officers whose details were discovered in this search. A response is then sent to the applicant and the other officers notified.

Scenario 10 — Granting Permission to Access Services
A member of the public wishes to access government services electronically for the first time. They apply for access and are given an appointment with an approved agent to establish their bona fides, and are then given the means to obtain access.

Scenario 11 — Enrolment of Government Employee
A new recruit to a Government Department arrives for the first day at work. They are brought onto the Departmental 'roll' and given the means to identify themselves electronically as a member of the Department.

Scenario 12 — Fraud Investigation
A government employee or agent is suspected of acting in a fraudulent or corrupt manner in association with partners outside government with whom he/she is in electronic communication. An investigation is launched which may require access to their transaction record without informing them.

Scenario 13 — Revocation of Government Employee
A government employee or agent is suspended or resigns and their authorities relating to their post are revoked.

Annex B
Example IAG Service Attacks and Threats

This annexe presents some example threats to the IAG service delivery with reference to the assets and threat agents identified. In considering whether a particular service offering might need to deal with such threat, the actual risk of attack needs to be considered. If the asset value is low, the impact small, or the technical difficulty of mounting the attack is high, it may not be necessary to install specific countermeasures.

Threat Notes

T1 — Unknown Outsider Attack
A hostile outsider may gain direct access to the IAG services with the objective of achieving some personal gain or causing damage to the system. The generally accepted 'hacker' attack from outside seeking to commit fraud or disruption. Examples might include fraudulently altering information held to the detriment of other transactions or the continuing provision of the service.

T2 — User Fraud
A legitimate user of IAG services may submit a false transaction or deny obligations in respect of transactions submitted. The generally accepted threat arising from dishonest customers. An individual may have been legitimately granted rights to use the system and tries to abuse that position. In most cases, measures against this sort of threat are more of a business application requirement than a security requirement. Examples might include submitting multiple benefit claims and/or denying responsibility for fraudulent claims submitted and subsequently detected.

T3 — Insider Attack
An individual with privileged access to government data networks may abuse that position to create false transactions or interfere with legitimate transactions. The generally accepted 'insider' attack from other parts of government not directly connected with the service. Examples might include 'hacking' attacks from inside government networks on the more privileged inter departmental elements of the services. Note that the attack may actually originate from outside following a breach of the defences to the IAGSPD.

T4 — Privileged Insider Attack
An individual with privileged access to or management responsibility for IAG service provision may abuse that position to interfere with or exploit service provision. The generally accepted 'insider' attack from operational staff responsible for the system. Examples are the traditional fraudulent use of privileged capabilities to alter records, create false accounting trails, or create phantom users.

T5 — False Identity
An individual may establish false or multiple identities to access IAG services and submit fraudulent claims or cause other damage to the service. All classes of threat agent may have an interest in creating false identities, insiders may find it easier than outsiders but are at greater risk. Examples exploitations might include submitting benefit claims using false bona fides.

T6 — Impersonation

An individual may impersonate a legitimate user or operator in order to secure services on that user's behalf. An outside may attempt to impersonate a user or system operator, either by forging or otherwise acquiring legitimate credentials and making representations on behalf of the legitimate user which might be difficult to disavow.

T7 — Unauthorised Disclosure
Personal information or other information submitted as part of an IAG transaction may be disclosed to those with no need or rights to access it. The generally accepted privacy or confidentiality threat. This could lead to a failure to comply with the DPA or the risk that the personal information gained could be used for fraudulent purposes and also undermine confidence in the service. Examples include the probing of the external networks for exploitable information such as payment credentials or personal information.

T8 — Revoked Rights
Those who have in the past possessed rights of access to IAG resources may misuse those rights after they have, or should have been, revoked. Threats arising out of the inability to ensure that users and system management rights are not properly terminated once they no longer need them. Examples might include misuse of the access rights of a deceased person or misuse of insider rights after the individual concerned no longer has the responsibilities that carry those rights.

T9 — Theft of Access Tokens
Access tokens that confer rights with respect to IAG services may be stolen and used for improper purposes. Should some form of access token be used to control access, there is a threat that lost tokens might be abused. Examples might include theft of tokens or information required to gain IAG access or validate transactions.

T10 — Duplication of Access Tokens
Access tokens that confer rights with respect to IAG services may be duplicated and copies used for improper purposes. A distinct threat from loss of tokens in that a token holder may be unaware that the token has been copied. Examples include forgery or attempted copying of authentication tokens.

T11 — Capture of Access Credentials
Access credentials may be captured and used for improper purposes. Here the term access credential refers to the information needed to gain access rather than any token which is the physical packaging of the credentials. There are several attack approaches that might achieve this including:

passive monitoring of the network and other communications channels in order to acquire the authentication transfers and determine the authentication credentials;

creation of a bogus IAG access point with the intention of deceiving an unwitting IAG access user into revealing genuine access credentials and other information;

Subverting the CND such that access credentials or other transaction material might be disclosed to the attacker

T12 — Denial of Service Attacks
Threat agents may seek to deny access to the IAG services by legitimate users. Typically a threat arising from external or internal attack — 'hacking' or 'cyber vandalism'. There are several attack approaches that might achieve that including flooding attacks that seek to stress the service, and attacks on the PND or IAGSPD which might prevent legitimate transactions from being properly routed to the service.

T13 — Misinformation and Propaganda
IAG services, and hence use of the service, may be undermined by laying a trail of false and misinformation which purports to carry the authority of government by virtue of its apparent association with the IAG service. A threat arising out of an attack on the integrity of information held within or issued by IAG with the aim of destroying confidence in the service. Examples might include the replacement of content of web pages with false information, or the alteration of purported origin, content, or authority of communications from IAG service providers.

T14 — Breach of Anonymity
Transactions that are required to be anonymous may be traced to their originator and the association misused. The primary example of this would be any use of IAG systems for services such as ballots or informer lines where anonymity of the transaction is required.

T15 — Breach of Accountability
Users of IAG services, and the departments offering the services, may not be able to be held accountable for attempted fraud or maladministration. A secondary consequence of a directed attack or fraud is that the system authorities may not know that such a fraud is taking place or what the extent is. Partially a business rather than security requirement, but security requirements will impact on the protection of raw audit information.

T16 — Failure to Recover Business Information
Information assets contained within the system may become inaccessible if the access credentials are lost or unobtainable. Information may be lost following equipment failure or malicious attack. A proper backup regime will permit recovery from such situations. Another concern here is where encryption is used as a mechanism to limit access to specific individuals and the access credentials are lost (eg the individual loses or forgets the key/password). In the absence of a proper business information recovery mechanism, the information asset could be lost.

T17 — Loss or Theft of Monetary Value
Monetary value owned by IAG systems may be improperly disbursed. This is a specific case of the generic threat of loss of assets where the assets represent monetary value. Financial accountability and control introduces extra requirements beyond the business needs to control information in general.

T18 — Challenge to System Veracity
It is possible that a user may disavow a transaction with a claim that the IAG system was imperfect. A general requirement to be able to show that systems are correctly installed

and operated and that any evidence generated by the system in support of a dispute is admissible.

Annex C
Model for Security Requirements Expression

This framework document uses the internationally recognised Common (evaluation) Criteria (CC) Protection Profile (PP) model as the vehicle for the definition of security requirements (see http://www.itsec.gov.uk/ for information on the CC project). The CC PP construct is defined for the expression of security requirements for an IT security product or system that is intended to be the subject of formal evaluation against the CC leading to certification of compliance with the PP requirements. This document defines the security requirements for a service rather than a product, the CC definition of the PP construct has therefore been adapted to describe a secure service whilst maintaining as far as possible the underlying CC model.

The CC Protection Profile is a structured representation of security requirements that can be certified as a suitable response to the security problem described. Part 1 of the CC explains the underlying model in some depth, figure C.1 below illustrates the PP concept.

[NOT AVAILABLE] Figure C.1, Simplified Common Criteria Protection Profile Structure

The Protection Profile presents the security requirements in terms of the following:

a. The Security Environment is a statement of the security problem by identifying the assets which are to be protected, the threat agents who might represent a threat to those assets, and the specific threats to those assets. A threat is a particular attack that exploits asset vulnerability.
b. The Security Objectives are a concise statement of a set of control objectives which, when achieved, will result in the required level of protection being achieved.
c. The Security Requirements are a set of technical security requirements statements against which any implementation can be tested.

The aim of the profile model is that it should be possible to show proper traceability from the environment (statement of the problem) to the objectives and thence to the detailed security requirements statements. The profile will be supported by a rationale that demonstrates that the security requirements are a complete, effective, and cohesive solution to the security problem described.

This framework document currently makes no reference to the CC part 2 security components and packages, security requirements are expressed in narrative form. Any adaptation to the needs of the evaluation community has been deferred until the principles and narrative content have been adopted as the basis for service provision and the detailed security requirements for the major elements of the security services have been determined.