

INFORMATION ASSURANCE POLICY

For

NORTHERN IRELAND CIVIL SERVICE

Version 1.0

18 May 2009

DF1/08/295407

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

CONTENTS		Page
	Glossary	5
1	Executive Summary	6
2	Introduction	7
3	Background	9
4	Risk Management / Accreditation of Systems	13
5	Information Assurance in NICS	15
6	Sources of Guidance	17
7	Recent Government Directives	20
8	Maintaining Information Assurance in NICS	23
Appendix 1	Key Elements of Information Assurance Roles	25
Appendix 2	Reminders for all Users	27
Appendix 3	Information Assurance Training	28
Appendix 4	Contact Information	29
Appendix 5	List of NICS Policies	30

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

IA Policy	Version 1.0
DID Reference	DF1/08/295407
DATE	18 May 2009
AUTHOR	Information Assurance Team
OWNER	NICS Accreditation Panel

Version Control

Version 0.1	Redraft by DID Information Assurance Team for review by Work Group on 24/9/08
Version 0.2	For review by NICS SIRO
Version 0.3	For review by Work Group on 19/ 2/09
Version 0.4	For approval by NICS Accreditation Panel
Version 1.0	Approved for issue by NICS SIRO 18/5/09

Members of Working Group

Fiona Brashaw, DID
Gerry Beck, DID
Colin Cluney, DID
Colin Honeyford, DRD
Kevin Meenan, DSD
Lorraine McEvoy, DID
Roisin McKay, DEL
Roger Millar, NIO
Brian O'Doherty, ITAssist
Lewis Taylor, DFP
Margaret Taylor, DID

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

GLOSSARY

BPSS	-	Baseline Personnel Security Standard
CESG	-	National Technical Authority for Information Assurance
CIA	-	Confidentiality, Integrity and Availability
CINRAS	-	Comsec Incident Notification Reporting and Alerting Scheme
CLAS	-	CESG Listed Adviser Scheme
ComSO	-	Communications Security Officer
CSIA	-	Central Sponsor for Information Assurance
DEL	-	Department for Employment and Learning
DFP	-	Department of Finance and Personnel
DID	-	Delivery and Innovation Division, Department of Finance and Personnel
DPA	-	Data Protection Act, 1998
DRD	-	Department for Regional Development
DSD	-	Department for Social Development
DSI	-	Directorate of Security and Intelligence
DSO	-	Departmental Security Officer
FIA	-	Freedom of Information Act
GSi	-	Government Secure Intranet
HRMS	-	Human Resource Management System
IA	-	Information Assurance
IAO	-	Information Asset Owner
ICO	-	Information Commissioner's Office
ICT	-	Information and Communication Technology
IL	-	Impact Level
ITSO	-	IT Security Officer
MPS	-	Manual of Protective Security
NDPB	-	Non Departmental Public Bodies
NICS	-	Northern Ireland Civil Service
NIO	-	Northern Ireland Office
NSG	-	National School of Government
OFMDFM	-	Office of the First Minister and Deputy First Minister
PMQ2	-	Protective Marking Questionnaire v2
PSN(R)	-	Public Service Network (Restricted)
RMADS	-	Risk Management Accreditation Document Set
SAU	-	Security Advisory Unit
SIRO	-	Senior Information Risk Owner
SO	-	Cabinet Office Official Committee on Security
SPF	-	Security Policy Framework
SRO	-	Senior Responsible Owner
UKITSO	-	UK IT Security Officer

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

1 EXECUTIVE SUMMARY

This document sets out the requirements for information assurance in NICS relevant for the ongoing modernisation in the Service and in line with the [2007 National Information Assurance Strategy](#). This Strategy outlines an approach for the UK in adopting information risk management by ensuring the right level of professionalism, education and training and availability of IA products and services, as well as compliance and adoption of relevant standards. Information is an important business asset and this policy is intended to ensure that information assurance is at the core of business processes.

The policy places particular importance on the assessment and management of risks, clear accountability for such and ownership at Board Level. This document includes a description of key roles necessary for maintaining information assurance including the roles of Senior Information Risk Owner, Information Asset Owner and Accreditor.

Accreditation is defined as 'the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users'.

The policy specifies the requirement for systems to be the subject of an accreditation process and describes the arrangements for the accreditation of systems which provide services across all the Departments.

The policy also places high importance on appropriate security training for staff at all levels and, in addition, specialist training for those with specific security roles.

This policy replaces the NICS Public Service Network Community Security Policy and Code of Connection (February 2006). The Code of Connection requirements for the present infrastructure in NICS have been revised and are now detailed in a separate document entitled "Code of Connection for Northern Ireland Civil Service Networks".

This Information Assurance Policy is owned by the NICS Accreditation Panel who will be responsible for its maintenance and review. It has been authorized for release by the NICS SIRO, who is the Chair of the NICS Accreditation Panel. The NICS Accreditation Panel may, at its discretion, commission work to develop detailed guidance on specific topics.

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

2 INTRODUCTION

The need for citizens and organisations to have confidence in the ability of the Northern Ireland Civil Service (NICS) to manage information securely has never been greater, particularly as information is increasingly shared between organisations and systems are increasingly interconnected.

Public services within Northern Ireland depend on the availability and accuracy of information within government systems. The NICS is committed to maintaining governance arrangements and procedures which will enable the proper management of risk to information and has clear lines of accountability for such.

This document provides advice on current policy in NICS for maintaining information assurance, the term given to the management of risk to information.

This document supersedes the NICS PSN Community Security and Code of Connection dated February 2006.

The guidance in this document is relevant to everyone involved with the planning, designing, delivery and implementation of ICT systems and services in the NICS including Senior Information Risk Owners (SIROs), Departmental Accreditors, IT Security Officers (ITSOs) and Information Asset Owners (IAOs), as well as all users of all systems. A review of the various roles is contained at Appendix 1. Useful reminders are also listed at Appendix 2.

Whilst the main focus of this document is on information assurance from the ICT perspective, it is recognised that information can be held in various other formats including paper records, CDs etc. Specific advice on the handling and storage requirements of such material is available in the revised publication 'Guide to Document and IT Security'.

The objectives of this policy document are to –

- Establish a policy which is both up-to-date with recent government directives for information assurance, and relevant for the evolving ICT landscape across the NICS, in which shared services are central;
- Explain the fundamental principles and requirements for information assurance;
- Promote understanding of information assurance as a business enabler;
- Describe the existing arrangements and requirements for maintaining information assurance in NICS; and,
- Highlight fundamental security requirements relevant to all staff in the NICS.

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

The NICS is committed to delivering high quality, effective and efficient services which meet the needs of citizens and customers and will continue to exploit the most appropriate technology to assure public good. Information assurance is critical to the success of these efforts and everyone without exception has a part to play.

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

3 BACKGROUND

Adequate protection of information and systems is necessary within public sector systems, not only to protect national security but also to assure the public that we are protecting their sensitive details. Whilst it is necessary to comply with legislative requirements, it is also necessary to deliver modernised services to the community and to increase the uptake of on-line services.

The potential threats to information systems are varied and can range from theft of equipment to such criminal activity as hacking into a website and defacing it, or online identity fraud e.g. phishing, to deceive persons into disclosing credit card numbers, bank account details or other valuable information. Threats also include human error and malicious activity.

3.1 Definition of Information Assurance

Information Assurance is defined in HMG IA Standard No 2 Risk Management and Accreditation of Information Systems (v 3.1 October 2008) as 'the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users'.

Determination of the measures to protect a system and the information it holds must take into account the confidentiality, integrity and availability of the information as defined below –

- **Confidentiality** – ensuring that information is only available to those who are authorised to access it
- **Integrity** – to safeguard the accuracy and completeness of information and the methods that are used to process it
- **Availability** – ensuring that users have access to the data and/or systems as and when required.

These three facets of information are often referred to as '**CIA**'. The measures to protect information normally include a combination of physical, technical, personnel and procedural controls.

3.2 Legislation

Under the Data Protection Act 1998 there is a legal requirement to ensure that personal data is held accurately and securely and in accordance with the principles of the Act. Other relevant legislation includes, but is not restricted to, the following:

- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

- The Freedom of Information Act 2000
- The Official Secrets Act 1989
- Human Rights Act 1998
- Regulation of Investigative Powers Act 2000

With increasing dependency on ICT systems, the availability aspect of information systems is increasingly significant, hence the importance of business continuity planning.

3.3 The Environment for Security

Government departments are required to provide a comprehensive protective regime in line with the good practice guidance in ISO/IEC 27001 in order to establish and maintain a secure environment for the protection of information. Key elements of this are:

- Clearly defined roles and accountability for ICT security
- Appropriate vetting of staff and contractors
- Controls based on cost effective assessment of risk
- Training awareness for staff
- Relevant policies and procedures
- Mechanisms for monitoring and reporting security incidents
- Business continuity planning

For many years the above have all been recognised as essential strands in a good security regime. With increasing sophistication in technology and the establishment of shared services and joined up government, particular emphasis is now placed on accountability for effective risk management and a requirement for information risk management to be a core function and an integral part of the business decision process.

The importance of security awareness for all levels of staff cannot be over stated. Staff should familiarise themselves with the content of the NICS Information Assurance online training package at the earliest opportunity. While staff do not need to be technical security specialists, they must ensure they are familiar with the security policy / security operating procedures for the systems they use.

Information on specific training requirements can be found at Appendix 3.

Increased importance is now placed on effective monitoring of systems and on the timely application of software patches from suppliers. CESG Infosec Memorandum No 22 Protective Monitoring provides details on this requirement.

The NICS is currently taking forward work on identity and access management technologies. It is important that identity information and access rights are properly aligned with business requirements and that only valid users have access to applications and data that they are authorised to access. Access control measures

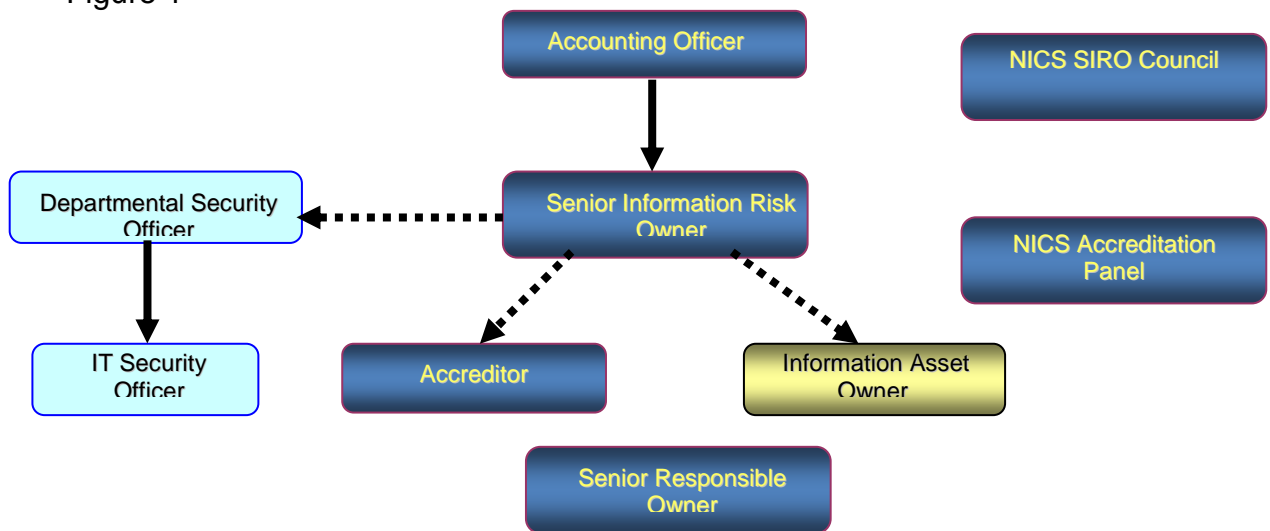
NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

must be documented within the security operating procedures for a system. Responsibility for access rights to system data should be clearly defined and be regularly reviewed and audited.

Shared information is information that is owned by one business unit and is passed, copied or sent to another business unit to assist them in their business objective. Information can include all forms of media, both paper based and electronic. Access to information should be limited to those with a need to know. Shared information should be handled and stored with care, and used under conditions that make accidental or opportunist compromise unlikely and which deter deliberate compromise in line with the requirements of the Data Protection Act 1998.

The Central Sponsor for Information Assurance (CSIA) advise that departments should have a Senior Information Risk Owner (SIRO), Departmental Security Officer (DSO), Accreditor, IT Security Officer (ITSO) and Information Asset Owners (IAOs). Definitions of the roles of these posts can be found at Appendix 1 and the relationships are shown in Figure 1.

Figure 1



3.4 Classification of Information

Within government the Protective Marking Scheme is used to aid with the determination of the controls that are necessary to adequately protect, store and transmit data. The different markings (in ascending order) are:

- Protect
- Restricted
- Confidential
- Secret
- Top Secret

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

It is important that the correct marking is applied to data in accordance with the guidance contained in the Security Policy Framework (SPF) as the marking will be used within the accreditation process to determine appropriate controls.

Within the NICS, the PMQ2 questionnaire has been produced as a handy guide for determining the correct classification of data.

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

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

3.5 Security Clearance

Departments must ensure that all staff with access to Government networks or systems as a minimum comply with the Baseline Personnel Security Standard (BPSS). This also applies to temporary staff and contractors.

Departments and Agencies must ensure that ICT users with higher levels of privilege and/or potentially wide access (e.g. system administrators) or those with responsibility for ICT security must be subject to evaluation for National Security clearances appropriate to the protective marking of the information processed and relevant GSi requirements.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

4 RISK MANAGEMENT AND ACCREDITATION OF SYSTEMS

All departments and agencies must achieve effective protective security through the application of risk management in accordance with the guidance in HMG IA Standard No 1 Technical Risk Assessment.

Systems which handle government data must be accredited using HMG IA Standard No 2 Risk Management and Accreditation of Information Systems and the accreditation status must be reviewed at least annually.

Accreditation is the formal assessment of Information System assets against Information Assurance requirements. The process of accreditation ensures that the risks to the assets have been accurately evaluated and that the protective security strategy for the assets is cost effective and commensurate with risk.

In assessing the level of impact likely to result from any compromise of information assets, Departments and Agencies must use 'Business Impact Levels' (ILs) as specified in HMG IA Standard No 1. ILs provide a seven point scale which allows Departments and Agencies to make a balanced assessment of the countermeasures to meet risk management requirements for Confidentiality, Integrity and Availability. In addition, Departments must consider where large amounts of data are aggregated to determine whether a higher impact level applies and therefore greater protection is needed.

The NICS network operates at IL3; however, individual systems may be assessed at a higher specific 'CIA' level and thus require additional risk mitigation measures.

The Accreditor is responsible for granting permission to operate the system according to conditions agreed between the Accreditor and the System Owner on the basis that risk has been assessed, is being managed and does not present an unacceptable level of risk. The risk assessment and the conditions on which accreditation has been granted, together with the security policy and security operating procedures, should be included in the security documentation, known as the Risk Management Accreditation Document Set (RMADS), for the system. It is normal practice for project managers to engage the services of a CLAS¹ consultant to provide independent advice on how well risk has been assessed and the adequacy of the controls. In many cases the Accreditor will mandate this. In addition the adequacy of the controls should be tested at appropriate intervals, as agreed with the Accreditor, by companies qualified under the CESC Check Scheme to carry out Health Checks and identify any vulnerabilities that could be exploited.

For all new systems within the NICS an Accreditor must be involved from the concept stage onwards. The Project Board in consultation with the Departmental Accreditor should agree who fulfils the role. It is most important that departments seek advice on risks from persons who are qualified and approved to provide advice.

¹ CESC Listed Adviser Scheme

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

The Accreditor and the Information Asset Owner (who may also be the System Owner) are responsible for ensuring that the accreditation status of the system is reviewed at appropriate intervals, normally yearly, and at times when there is significant change to the system.

Adequate documentation supporting the Accreditor's decision should be retained.

Risk management involves everyone playing their part in complying with policy and procedures, and should be a key feature of regular Information Assurance audits.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

5 INFORMATION ASSURANCE IN NICS

In recent times there have been radical changes in ICT across the NICS. Each Department is playing its part in the most significant change in ICT provision for over twenty years. While continuing to perform its particular business activities, each Department is seeking to realise the benefits of Shared Services i.e. AccountNI, HRConnect, RecordsNI and ITAssist. Each of these services is delivered across a new wide area network, NetworkNI, serving the whole of the NICS. Departments are now more interconnected than ever before and ICT services more interdependent.

The role of the Accreditor in Departments is to act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the Department. This has always been the case for line of business² systems and for individual Departmental IT Networks.

With the introduction of NetworkNI, the emphasis for the Accreditor will not only be on line of business but also on how the owners of line of business services and common services are both provided with the requisite information assurances, and the overall level of network assurance is risk managed for mutual benefit.

Clearly there is no reduction in the responsibilities of the individual Accreditor as the introduction of a range of ICT-enabled shared services, including NetworkNI, IT Assist, HR Connect, AccountNI and RecordsNI introduce new shared responsibilities and a greater requirement for careful thought when scoping or defining the accreditation boundaries.

The accreditation scope may be defined in a number of ways: business (organisational, functional), physical (site, computer, network), logical (connectivity, service, software), contractual (an outsourced system or service), or a combination of these.

The following table illustrates how systems / services might be grouped according to the level of trust that could be placed on them.

Systems / Services involved	Examples
Systems owned by the organisation for which it has full responsibility and over which it has direct management control.	A network that is internal to the business.
Systems outside the direct control of the organisation but controlled by other organisations with whom there is a trust relationship based on formal compliance.	Shared assets or services. Connection to centralised services and networks such as GSi. The Government Gateway.

² Line of business may be defined as the activity for providing the services of a particular department

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Where an organisation has put in place contractual controls with a third party to manage their information system.	Any service outsourced to a third party.
Systems outside the direct control of the organisation where limited trust may be enabled by standard commercial contract conditions.	Standard services offered by commercial communications bearers.
Systems over which the organisation has no control.	The internet, public communications networks.

All parties concerned must be clear about what is being accredited and understand the business context for accreditation. When scoping or defining the accreditation boundaries of an information system, governance must be established which will include the management of risk and accreditation accountability.

Security Implications for Managed Services

The division of responsibility for security matters must be clearly defined between Departments and the Service Provider. With reference to figure 1, the departmental Accounting Officer, as the service customer, is advised by the SIRO, IAO, local IT Security Officer and DSO, with additional support from the Information Assurance Team of DFP's Delivery and Innovation Division (DID) and a CLAS consultant where necessary, and is responsible for defining and agreeing the security requirements within the overall requirements for the system / service and ensuring that the security requirements are included in the final contract.

The Service Provider will normally be responsible for:

- complying with agreed security policy including the requirements for security clearance for staff involved with contract
- carrying out security risk and management reviews as part of design, implementation of service, change control and monitoring and review
- implementation of appropriate protective measures including contingency plan
- day-to-day monitoring of protective measures and reporting to departments
- awareness training of provider's own staff.

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

6 SOURCES OF GUIDANCE

The [Security Policy Framework](#) (SPF) issued in 2008 by the Cabinet Office Security Policy Division on the authority of the Official Committee on Security (SO) replaces the Manual of Protective Security and is available to NICS as guidance and good practice.

6.1 Procedures within NICS

Within NICS there are procedures which address such matters as [use of internet and email](#), use of laptops, [blackberry devices](#) etc. Staff must comply with those procedures which are relevant to their work. Managers of new projects and technologies must arrange for documented procedures to be available for end users and should involve the Information Assurance Team where appropriate in the development and revision of such procedures. Following the completion of the Data Handling Review in NICS there will be a review of policies and procedures to ensure existing ones remain appropriate and in line with the current requirements of NICS. Staff should consult their local IT Security Officer for advice as required.

6.2 Code of Connection Requirements

The detailed requirements for the network connections required for NICS to deliver services are contained in a separate document entitled “Code of Connection for Northern Ireland Civil Service Networks”. It is essential for information assurance that all connecting networks meet the requirements in this Code of Connection. Compliance with the detailed requirements specified in the Code of Connection for Northern Ireland Civil Service Networks will enable a good measure of trust in the security provision of connecting systems/organisations.

6.3 Data Sharing

At the heart of the Government’s Information Sharing Vision Statement of September 2006 is the desire to provide more customer focused services. [The Data Sharing Review](#)³ has highlighted the public value delivered by the appropriate sharing of sensitive information. When considering data sharing proposals, Departments must ensure that they are compliant with Data Protection (DPA) and Freedom of Information (FOI) regulatory requirements. A key component within an appropriate data sharing framework is a Privacy Impact Assessment which needs to be carried out. The Information Commissioner’s Office (ICO) (details at www.ico.gov.uk) can provide relevant guidance.

6.4 Cryptography

Departments and Agencies must comply with HMG Information Assurance Policy No 4 Communications Security and Cryptography (parts 1-3) for the protection of protectively marked material.

³ Data Sharing Review dated 11 July 2008 by Richard Thomas and Mark Walport

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

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

6.5 International Security Agreements

Departments and Agencies engaged in sensitive work with international organisations, or those that handle protectively marked information on their behalf, must ensure that their internal procedures are compliant with the relevant international obligation (e.g EU Directives) and be cognizant of requirements under both the Data Protection Act 1998 and European Commission Directives.

6.6 Bodies in NICS which have a Specific Role in Information Assurance

6.6.1 The NICS Accreditation Panel

The NICS Accreditation Panel was established in June 2000. Until recent times its main focus was maintaining the integrity of the Public Service Network in NICS, known as PSN(R) or the NICS Backbone, by accrediting the connection of departmental networks and a number of interdepartmental systems, such as HRMS, in order to ensure that the standards required for the protection of NICS data, and the NICS connection to GSi, were maintained.

The Panel is chaired by the Senior Information Risk Owner (SIRO) for NICS and comprises the Departmental Accreditors and other senior managers. The Panel now meets at least quarterly to deal with issues arising from the Reform Agenda and the introduction of NetworkNI, AccountNI, HRConnect, RecordsNI and ITAssist.

The Panel is the final accrediting authority for common systems connected across NetworkNI and normally requires the Senior Responsible Owner (SRO) to confirm that a Health Check has been conducted and that its recommendations have been implemented. A written statement from a CLAS consultant, stating his/her opinion on the assessment and management of risk, is also required before accreditation is considered. Most of the major projects have a security committee to oversee the preparation for gaining and maintaining accreditation.

6.6.2 Departmental IT Security Officers

Departments have their own IT Security Officer who supports the Departmental Security Officer. An overview of the role of the ITSO is at Appendix 1.

6.6.3 Information Assurance Team

The Information Assurance Team within Delivery and Innovation Division provides support to the NICS Accreditation Panel and advises and assists departments with various activities in preparation for accreditation. The Information Assurance Team liaises with CESG when there are requirements for specialist advice and

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

consultancy and they represent NICS at the UK IT Security Officers Forum and the UK Accreditors' Forum.

6.6.4 The ITSO Forum

The ITSO Forum is made up of ITSOs from all NICS core Departments including the NIO, as well as from a number of NDPBs and other Agencies. The Forum provides an opportunity for Departments to share information and experiences, to promulgate policy and to extend awareness. The Forum is supported by the DID Information Assurance Team (formerly the IT Security Team) which also provides feedback from the UKITSO Forum and the UK Accreditors Forum.

6.6.5 Security Advisory Unit

The Security Advisory Unit (SAU) is part of OFMDFM and its overall function is to promote an effective regime of personnel, physical, document and asset security within the NICS. Their key responsibilities include personnel vetting policy and maintenance of the vetting regime across NICS departments, receipt and dissemination of protective security and terrorist threat information, physical security surveys and audits, advice to departments regarding security provisions in contracts and the provision of assurance to Head of Civil Service on the efficiency and effectiveness of the protective regime in NICS on an annual basis.

6.6.6 The Senior Information Risk Owner for NICS

This officer is the focus for the management of information risk across the NICS, represents the NICS at joint SIRO events in Whitehall and is the contact with the Cabinet Office for driving forward security initiatives in the NICS and for reporting security matters as required to the Head of the Northern Ireland Civil Service (HOCS) and Permanent Secretaries/ Minister. As stated earlier the NICS SIRO chairs the NICS Accreditation Panel.

6.6.7 Crypto Custodian

The role of the crypto custodian is to ensure compliance with HMG and NICS policy and procedures governing cryptographic items under their control, and taking responsibility for the management and accounting of all cryptographic material.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

7 RECENT GOVERNMENT DIRECTIVES

Following the Data Handling Review of 2007/2008 the Cabinet Office mandated Whitehall Departments to follow up action in the following areas:

- Departments to appoint an Information Asset Owner, and to review all data held and implement appropriate safeguard measures
- Information risk awareness training
- Reporting of breaches of classified data
- Forensic readiness
- Annual assessment of the effectiveness of Information Risk Management

The remainder of this section outlines the directives from the Cabinet Office. As stated in paragraph 6.1, NICS will develop policies and procedures which take into account the findings from 2008 NICS Data Handling Review and also consider the directives from Cabinet Office and those contained within the Strategic Policy Framework (SPF), where the principles are relevant to the situation in NICS.

7.1 Information Asset Owners and Review of all data within Departments

The Cabinet Office requires that all HMG departments establish Information Asset Owners. These officers will be responsible for risk assessments of the assets within the relevant business areas and putting in place safeguards to mitigate the risk of compromise.

7.2 Information Risk Awareness Training

The Cabinet Office has stipulated that all government staff regardless of grade who handle personal protected data must undergo training in order to ensure that they understand its value and the potential implications of their actions, and also to encourage behaviours where staff value, protect and use data for the public good. The Cabinet Office has advised that the delivery of the training should be by e-learning supplemented as appropriate for local needs.

Appendix 3 provides an overview of the different Information Assurance training requirements.

7.3 Reporting of Breaches of any Classified Data

The organisations listed below need to be informed about significant information security incidents. The contact details are available in Appendix 3. Currently within the NICS it is the responsibility of the Departmental IT Security Officer to report security incidents and to notify the Departmental Security Officer and Departmental SIRO of such. If the incident has potential implications for other NICS departments

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

(or indeed external organisations), the NICS SIRO should also be informed at an early stage.

- All significant breaches of classified data must be reported to the Directorate of Security and Intelligence (DSI) Secretariat at dsi@cabinet-office.x.gsi.gov.uk
- All incidents of electronic attack, actual or suspected, should be reported to GovCertUK. This includes: significant effect of virus resulting from malware, disruption of service, and other events that may reflect electronic attacks whether attempted or successful. Minor incidents such as receipt of SPAM need not be reported.
- Incidents involving cryptographic equipment and/or the associated key material (e.g. encrypted laptops, secure telephones) should be reported to CINRAS (the Comsec Incident Notification Reporting and Alerting Scheme) at cinras@cesg.gsi.gov.uk due to the inherent sensitivity of cryptographic items.

If an incident occurs which involves the loss or possible loss of personal data where there are Data Protection Act implications, the Data Protection Officer in the department should also be consulted as he/she will be able to advise on further considerations and actions required.

The Information Assurance Team within DFP Delivery & Innovation Division are available for advice where required.

7.4 Forensic Readiness

The Cabinet Office has recently highlighted the benefit of forensic readiness which is the capability of a department to use digital evidence in a forensic investigation such as:

- Unauthorised access to or tampering with ICT systems
- Fraud or other criminal activity
- Commercial disputes e.g. intellectual property rights
- Disciplinary issues
- Privacy issues e.g. compliance with the Data Protection Act

In practice, this will require departments to have high level procedures in place to advise on who to contact in the event of any incident which may require digital evidence to be preserved for further investigation by the appropriate bodies.

7.5 Annual Assessment by Internal Audit

Internal Audit should carry out an annual risk based review of information assurance, including the various roles (SIRO, IAO, DSO, ITSO & Accreditor), effectiveness of policies and procedures and compliance with best practice. Findings and recommendations should be brought to the attention of the Audit

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

Committee and the Head of Internal Audit should refer to Information Assurance in his/her annual assurance statement to the Accounting Officer.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

8 MAINTAINING INFORMATION ASSURANCE IN NICS

8.1 Maintaining the Accreditation Status for Common Systems

HMG IA Standard No 2 (Risk Management and Accreditation of Information Systems) dated October 2008⁴ provides the overarching governance concepts, process and documentation associated with accreditation of systems. It provides clear correlation between the delivery of a project (be it delivering a common or line of business system) and the risk management processes that need to be employed to ensure adequate information assurance is delivered.

Governance arrangements in the NICS are centred on departments being responsible for the accreditation of their line of business systems.

The NICS Accreditation Panel, on the other hand, has overall responsibility for accrediting shared systems and has been involved at various stages during the development of these projects in overseeing the preparation for interim accreditation and/or full accreditation as appropriate.

Arrangements for maintaining the accreditation status of these services must be planned for, particularly as the original project teams will inevitably disperse and the respective project boards are likely to meet less often. The Project Boards for these shared systems, in consultation with the DFP Accreditor and the Head of Contract Management section, or the NICS Accreditation Panel, where appropriate, must take responsibility for agreeing the process which will enable the accreditation of the systems to be reviewed whenever changes are planned for the system, otherwise annually. The agreed process and responsibilities should be notified to both the NICS Accreditation Panel and the Permanent Secretary in Department of Finance and Personnel.

8.2 Information Assurance within Departments

The Permanent Secretary in each department is responsible for the arrangements for Information Assurance within the department and identifying clearly the appropriate levels of Information Assurance that need to be attained and maintained for each line of business system, where the requisite Information Assurance responsibilities lie, including the relationship between the Department's Management Board and the Boards of agencies and other bodies. It is essential that Information Assurance roles and responsibilities are clearly defined and that the Permanent Secretary satisfies himself/herself that the risk to information is being appropriately managed and, importantly, there are appropriate reporting lines as well as effective mechanisms for monitoring risks to information. Departments and Agencies must have a designated Senior Information Risk Owner and Information Asset Owners, whose main responsibilities lie in the delivery of the requisite level of Information Assurance for their individual organisation, and Departmental Security Officer (DSO) with day to day responsibilities for all aspects of Protective Security (including physical, personnel and IT security).

⁴ [HMG IA Standard No 2 – Risk Management & Accreditation of Information Systems](#)

NICS Information Assurance Policy (NOT PROTECTIVELY MARKED)

There should be an Information Asset Owner for each system who understands all the information held and is responsible for risk management. This officer would normally be the senior officer who commands the business unit. In addition departments should have an Accreditor. Appendix 1 specifies the core responsibilities associated with the Accreditor and Information Asset Owner roles. Departments and Agencies must adopt a risk management approach (including a detailed risk register) to cover all areas of protective security across their organisation.

They must also have a designated Information Technology Security Officer (ITSO) responsible for information in electronic form. In addition, if a department handles cryptographic material, there should be a designated Communications Security Officer (ComSO).

Departments and Agencies must have a system of assurance that provides the requisite compliance with Information Assurance policy, reports the level of compliance to their Accounting Officer / Management Board on the state of all aspects of Information Assurance.

The recommendation of the NI Data Protection Review specially notes the requirement to establish a target for Information Assurance and an appropriate action plan to ensure that the target levels of Information Assurance are met. It recommends use of an Information Government Framework and notes the requirement for Accounting Officers to include Information Assurance within their annual Statement of Internal Control.

8.3 Training and Awareness for Staff

Information assurance awareness and the requirement for increased professionalism featured prominently in the National IA Strategy 2007, and more recently the Cabinet Office mandated training for all levels of staff who handle personal information in government departments. In addition to encouraging staff to study the content of the NICS online training package at the earliest opportunity, managers should consider other measures which will help foster a culture of valuing and protecting information.

With increasing importance on the management of risk to ICT systems, it should be mandatory for staff with specific roles in information assurance to attend the courses needed to maintain competencies and skills, and these staff should be encouraged to obtain relevant professional qualifications.

Appendix 3 gives more detail on training for specific roles.

8.4 Reporting of Incidents

Departments must have mechanisms in place to allow for independent and anonymous reporting of Information Assurance/IT Security incidents.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Appendix 1

Key Elements of Information Assurance Roles

1. Role of Senior Information Risk Owner (SIRO)

- a) member of Management Board who takes ownership of information risk
- b) ensures an organisation structure is established for the delivery of effective information assurance
- c) ensures funding is available to train staff who have information assurance responsibilities
- d) ensures corporate security policies are produced and maintained
- e) ensures appropriate contingency planning is in place.

2. Role of Departmental Accreditor

- a) Responsible for the accreditation of line of business systems that operate in the department and provide statement recording such
- b) Makes decisions on further actions needed e.g. timing of Health Checks etc
- c) Provides direction on frequency of security reviews – normally annually depending on nature of business
- d) Represents the department on the NICS Accreditation Panel

3. Role of Departmental Security Officer

- a) Day to day responsibility for all aspects of Protective Security including physical, personnel and information security
- b) Implementation and dissemination of protective security policy
- c) decisions on personnel security matters
- d) guidance for incident reporting
- e) education and training.

NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)

4. Role of IT Security Officer (ITSO)

- a) Advises Accreditor on the accreditation of information systems
- b) Oversees the accreditation process within department
- c) Acts as Incident Response Handler in the event of a major incident affecting information systems in the department
- d) Provides advice and guidance to department and agencies to ensure they are compliant with IA policy
- e) Assists with information assurance awareness for all staff
- f) Reports to the Departmental Security Officer (DSO) on ICT security matters

5. Role of Information Asset Owner (IAO)

- a) Knows what information the asset/system holds, who has access and for what purposes
- b) Understands and addresses risk to assets
- c) Approves and minimises transfers of information whilst achieving the business purpose
- d) Approves arrangements for transfer of data e.g. on removable media
- e) Approves disposal mechanisms

6. Role of Senior Responsible Owner (SRO)

- a) Ensures that a system meets its objectives as agreed with the SIRO and IAO
- b) Understands the risks to the system, is aware of the overall risk and how the risks may affect strategic goals.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Appendix 2

Reminders for all Users

- 1 Never without exception share your password.
- 2 Know the rules for handling the data in your care and ask to see any appropriate procedures.
- 3 Before making data available to anyone else make certain that you have the authority and legal right to release it.
- 4 Do not access data unless it is part of your job and you have a business need to do so.
- 5 Never give out any data over the phone or in any other way unless you are absolutely sure who you are giving it to and they are entitled to that data.
- 6 Always “lock” your computer when leaving your desk.
- 7 Never take data out of the office unless you really need to and have the permission to do so.
- 8 Keep your laptop or Blackberry secure at all times and be sure that you know the policy and procedures for their use.
- 9 Ensure you know the NICS policy for email and use of the Internet
- 10 Be on your guard for SPAM email which asks you to disclose personal information including your bank or credit card details
- 11 Know the rules for handling protectively marked information.

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Appendix 3

Information Assurance Training

1 Information Security Awareness

All staff must undertake the NICS online Training Package in all topics available. This will form part of the induction programme for all new entrants. Staff with privilege accounts or who manage/support information systems require additional training.

2 Accreditor

All Accreditors should attend at least a one day overview on the accreditation process. In addition, anyone involved in accreditation reviews on behalf of their Accreditor must attend the relevant courses at the National School of Government.

3 Information Risk Management

SIROs, Information Asset Owners and others with responsibility for information risk management must attend an appropriate Information Risk Management course.

4 Information Assurance Roles

All staff with specific roles in information assurance must attend the courses needed to maintain competencies and skills, and these staff should be encouraged to obtain relevant professional qualifications. This will apply to the Information Assurance Team in DID and to the departmental ITSOs. Further information on relevant courses and qualifications can be obtained from the [National School of Government](#) (NSG).

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Appendix 4

Contact Information

Directorate of Security and Intelligence (DSI) Secretariat

Email: notify dsi@cabinet-office.x.gsi.gov.uk

GovCertUK

General Enquiries:- enquiries@govcertuk.gov.uk

Incidents and Alerts:- incidents@govcertuk.gov.uk

RESTRICTED communications (GSI only) :- govcertuk@cesg.gsi.gov.uk

CINRAS

Email:- cinras@cesg.gsi.gov.uk

**NICS Information Assurance Policy
(NOT PROTECTIVELY MARKED)**

Appendix 5

List of NICS Policies

Asset Disposal Procedures

<http://itassist.nigov.net/itassist-asset-disposal-procedures.doc>

Asset Movement Procedures

<http://itassist.nigov.net/itassist-asset-movement-instructions.doc>

Blackberry Service Deployment, Use and Support Policy

<http://itassist.nigov.net/blackberry.pdf>

Guidance on Security of Portable Assets

<http://itassist.nigov.net/itassist-guidance-on-security-of-portable-assets.doc>

NICS Internet and Email Policy

http://www.dfpni.gov.uk/csc_2-03_nics_internet_and_email_usage_policy.pdf

NICS Clear Desk Policy

<http://dfponline.intranet.nics.gov.uk/clear-desk-policy>

IT and Document Security

<http://dfponline.intranet.nics.gov.uk/guide-to-document-it-security.pdf>