

Protecting Government Information

# Independent Review of Government Information Assurance

by Nick Coleman

Commissioned by the Cabinet Office

# Foreword from John Suffolk, Government Chief Information Officer

We are already on the journey to transform the way we use information technologies (IT) in government. We are sharing citizen data to expand opportunities for the most disadvantaged, to fight crime, to save lives and to provide better public services. We are joining up and sharing data, services, and systems everywhere not just in the UK but worldwide.

This new approach is helping to realise benefits on a vast scale, but it also brings new challenges. We need to know when, where and who we can share with, how we can connect safely and how we can protect our information from deliberate attack, disaster or error.

In the changed delivery environment we must make information assurance policy very simple. We need minimum security requirements with rules that everyone follows without exception. We need to know exactly what we are allowed to do and what we are not allowed to do. That gives us security that everyone can depend on.

We need to think edge-to-edge as we join up. We have to look at the whole picture and the interfaces at every point. We need to think in terms of snakes and ladders – the vulnerabilities and the safe steps. We need to know the implications of working in a joined up environment and connecting data and systems together.

We have to be able to measure how well we are doing, so we need independent accreditation that is consistently reported and shared across government so we know what we can trust.

We are at a fundamental crossroads: we are either going to be secure or we are not. It is a binary decision.

This report and its recommendations will help us to meet the challenges ahead.

John Suffolk.

# Synopsis from the Information Assurance Review

Government is transforming the way it delivers services, sharing information and connecting networks on an unprecedented scale. The risks are constantly changing. Information now needs to be protected much more rigorously against deliberate attacks, as well as errors and accidents. People need to know that the government is adequately protecting and appropriately using the information it holds.

The Central Sponsor for Information Assurance (CSIA) at the Cabinet Office has commissioned an independent review to assess whether in this rapidly changing environment the government's information and infrastructure is adequately protected against deliberate attack, disruption to services or loss of critical data.

The independent reviewer was asked to report back on:

- whether information assurance across government is adequate enough to provide stakeholder confidence in the government's information infrastructure
- whether information and services are protected in a timely and cost-effective way
- the extent to which information assurance will support the requirements of shared services and the *Transformational Government* agenda.

## How well is government doing?

In summary, the review identified that although measures are difficult to come by, most departments are investing significant amounts of money and effort in information security. However, these capabilities have developed in silos.

The challenge now is to enable joined up government, which means connecting to more environments and sharing more data in an environment that is increasingly more hostile.

Government departments are actively trying to address these challenges; however adequate mechanisms are not yet in place to support them in achieving this, which puts at risk the government's aspirations for service delivery enabled by technology.

In essence information assurance is progressing within departments; but in a joined up world, where data and services need to be connected and layers of trust need to be established, new thinking and mechanisms need to be put in place.

The findings in the main report summarise the current situation highlighting many areas of good practice and issues which need addressing. From this key recommendations have been drawn together these are listed below:

# Strategic recommendations

Government needs to have a comprehensive understanding of the risks it is facing, to put clear policies in place, to ensure those policies are being delivered and monitoring performance for compliance as well as being able to respond to incidents.

The current mechanisms and approaches need to be sharpened to assist government to deliver information assurance in the current and future planned operating environment.

## Key Recommendations:

1. The government creates a *vision* for information assurance and that this vision is incorporated into existing vision statements.
2. Provide a central facility for sharing *risk information* and a central information risk register based on risks experienced by departments and their agencies. Have the centre invest in a core capability to understand the information assurance risks facing government.
3. Mandate *board owners* to report quarterly on information risks and performance backed up by an annual audit of department's capabilities. Within this, establish clear metrics for managing performance of suppliers.
4. Provide the Prime Minister with a summary of information assurance across government and associated spending required to deliver cross government security associated with information assurance.
5. Enable one central mechanism for developing coordinated joint working for sharing best practice and establishing priorities across government.
6. Create clear mandatory *policy* rules on security across government. Define minimum standards that departments sign up to. Enable independent monitoring for compliance.
7. Tackle *identity management* challenges through mandating the use of privacy impact assessments. Specify standards of protection for identity registration, management and use in government and the wider public sector.
8. Mandate *professional certification* for those working in information assurance in every government department across key defined roles. Ensure stakeholders are educated on information assurance and what is expected of them.
9. Measure security through audit and monitoring to a defined standard. Mandate the reporting of incidents to a central monitoring team responsible for capturing incidents and ensuring investigations are conducted and lessons are learned.
10. Have an *independent oversight* capability retained by government who can be called upon to give independent oversight and advice on information assurance to give stakeholders confidence. Provide this capability in addition to the formal regulatory roles that exist outside government.

# Approach to the review

An independent review of information assurance activity was commissioned by the Cabinet Office in order to provide an unbiased view of Governments' capacity in this critical area.

The findings and recommendations have been drawn from a number of sources including interviews with stakeholders, attendance at committees and working groups, surveys and discussions with representatives from government departments. In addition there were discussions with some suppliers to investigate their perspective on the supply chain, which government depends on for delivery of its services.

All government departments were invited to participate in a survey and a representative sample of departments and agencies was assessed in more detail. The survey was structured in the same way as departments' capability reviews, with the topics being covered adapted to information assurance.

The review also drew on lessons learned and emerging good practice from governments internationally.

## About the Government Independent Reviewer

Nick Coleman is a leading authority on security and information assurance matters. He has led several organisations in the field of information assurance.

Most recently he established the Institute of Information Security Professionals, serving as its first Chief Executive. This body was set up to accredit security professionals around the globe.

Before that he led IBM's security services business across Europe, Middle East and Africa, and had earlier been in charge of commercial operations for their Business Continuity and Recovery Services division in the UK.

In 2005 he was appointed to the EU European Network and Information Security Agency where he serves as a member of their Permanent Stakeholders Group.

He was asked to undertake this review, as a follow-on from the work he did for the UK government in 2003/4, creating an overview of information assurance initiatives taking place in the public and private sectors.

For more information about the CSIA go to [www.cabinetoffice.gov.uk/csia](http://www.cabinetoffice.gov.uk/csia)

If you would like to comment on this summary paper, please contact:

CSIA  
2nd Floor  
26 Whitehall  
London SW1A 2WH

Or email us at [csia@cabinet-office.x.gsi.gov.uk](mailto:csia@cabinet-office.x.gsi.gov.uk)  
or direct to [nick.coleman@cabinet-office.x.gsi.gov.uk](mailto:nick.coleman@cabinet-office.x.gsi.gov.uk)

© Crown copyright 2007

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.

The material used in this publication is constituted from 75% post-consumer waste and 25% virgin fibre.