The contents of this submission are entirely my own personal opinions, they do not reflect the views, opinions or policies of my family; past, previous or future employers; or the political party I am a member of.

There are 3 fundamentals to Information Security which are currently lacking in the Australian Government: User Education, Public Key Infrastructure, and Audit.

User Education

The propensity of Government departments to utilise employees' familiarity with Personal Computer (PC) operating systems to avoid providing adequate training has lead to a culture of indifference when it comes to I.T. Security. The insecure habits that individuals have developed when using their computers at home are being carried over to the workplace and are not being addressed by line management, Human Resources or I.T. Security. This is also evident in applications developers and systems administrators that have insufficient security training to produce and manage I.T systems where information security is a primary consideration.

Public Key Infrastructure

The lack of a pervasive Public Key Infrastructure (PKI) within Government and made available to individuals for secure communications when dealing with Government, combined with a general lack of knowledge of and experience with PKI in general is of major concern. A significant majority of Internet users would not be able to describe how a digital certificate fingerprint should be used to verify a server's authenticity, nor would many of them question an expired or invalid certificate.

There are moves overseas such as the eEurope initiative to provide smart cards utilising PKI for secure access to health services, payments, public transport and many other services. The eEurope initiative is currently on track to meet it's targets set out by the governing body, it's progress has already been significant.

Audit

The function of the Defence Signals Directorate (DSD), the Australian National Audit Office (ANAO) and to an extent the National Office for the Information Economy (NOIE) in providing an effective audit framework is not being adequately fulfilled. The role of DSD in Internet gateway certification appears to have changed in the past 5 years from proscriptive, to prescriptive, to almost a rubber stamp. Likewise, the apparent culture of minimal surprise by the ANAO has reduced the potential for an effective I.T. Security audit being performed. The role of NOIE in an audit function is unclear at the moment, they are producing a large quantity of recommendations but do not appear to be providing any audit framework for verification of compliance.

This lack of audit effectiveness in Government is leading to private companies being contracted to provide I.T. Security advice and audit functions; however, there is no legislation requiring these companies to meet any particular standards when conducting audits.

The end result of these factors is that I.T. systems are not being correctly audited, security assessments are incomplete, risk statements are incorrect, and a false sense of security is the result.

Conclusion

The result of these three areas of concern in relation to the terms of reference are that there are very few individuals within Government which have the relevant understanding of I.T. Security to provide an adequate assessment of privacy, confidentiality and integrity of the Commonwealth's electronic data and information transmittal.

An increase in security education for employees, combined with appropriate guidelines for management, HR and I.T. Security departments is essential.

A uniform scheme for server and client certificates to be issued from a Government authorised Certificate Authority (CA), combined with sufficient education of software developers, employees and the general public about PKI is essential. A model such as the eEurope initiative may not be entirely applicable to Australia; however, there are many significant parts to the initiative that are definitely worthwhile undertaking.

There are few effective audit capabilities to review the I.T. systems to a sufficient level and few skilled programmers with the appropriate security background to influence security in systems development. An immediate review of the I.T. Security audit functions and performance of DSD, ANAO and NOIE is also essential.

The combination of User Education, Public Key Infrastructure, and Audit are fundamental to ensuring the security of the Commonwealth's electronic information.

Robert Rose
PO Box 684
Belconnen ACT 2616
Ph: 0417 270 793