STANDARDS
Australia

Inquiry into Cyber Crime

House Standing Committee on Communications

Standards Australia's
Submission in Response
June 2009

Contact:

Name: Anne Byatt
Relationship Manager
Ph: 02 9376 6185
Anne.byatt@standards.org.au

Standards Australia
20 Bridge Street
Sydney NSW 2000

Purpose

This submission seeks to highlight how standards can provide alternatives to/be complementary to legislation as well as provide guidance and certainty for industry where needed.

Standards Australia has the capability, where appropriate, to work with the House Standing Committee on Communications and the Department of Broadband, Communications and the Digital Economy (DBCDE) to address some of Australia's information security management needs with regards to standards. Standards have become an integral and essential element in the present business environment. Current Australian Standards in this space allow for a management system to be put in place along with a governance structure allowing for the efficient treatment and prevention of security incidents for the Australian community (please refer to Appendices A, B & C).

Background

Standards Australia as a Standards Development Organisation, not only coordinates standardisation activities, but develops internationally aligned Australian Standards® that deliver Net Benefit to Australia. We have developed standards across most sectors of the Australian economy, in traditional industries such as goods and services, engineering and construction, in other technical areas such as health and food, in emerging new areas of technology such as e-health, as well as in less technologically based subjects such as complaints handling and risk management.

Terms of Reference

Standards Australia will address the following terms of reference in our submission:

a) nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software as viruses and trojans;

b) The implications of these risks on the wider economy:
   - Including the growing economic and security impact of botnets.

c) Level of understanding and awareness of e-security risks within the Australian community.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:
   - Education initiatives
   - Legislative and regulatory initiatives
   - Cross-portfolio and inter-jurisdictional coordination
   - International co-operation.

Discussion

Standards Australia will address the terms of reference a), b) and c) together in one response.

a) nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software as viruses and trojans;

b) The implications of these risks on the wider economy: Including the growing economic and security impact of botnets.

c) Level of understanding and awareness of e-security risks within the Australian community

Better regulation means choosing the best regulatory instrument to achieve a policy outcome. This requires looking at risk. Better regulation strikes a balance between the risk to the community from the behaviour being regulated and the restrictions placed on the community and business. The instruments chosen will lie somewhere between self-regulation (where the risk is low) and detailed, black-letter regulation (dealing with high risk behaviour).

In this context, standards offer an alternative instrument of regulation, either on their own (a form of industry self-regulation) or as 'co-regulation', where standards are called up in generalised Commonwealth, state or territory acts or regulations. There are many types of standards, including Australian Standards from Standards Australia, standards produced by other organisations, industry codes that protect consumers, and other instruments. This includes the ASIC industry codes of practice and the ACCC codes of practice.

Consensus-based standards or codes have the key advantage that, rather than being imposed by government, sometimes with limited consultation, they are instead derived directly from consultation between stakeholders from the sectors affected, which includes government agencies and regulators. This extensive consultation should considerably improve the chances of the outcome being accepted by business and the community.

Better regulation is about regulatory options, which should strike the right balance between protecting the community and economy against risk, protecting rights, serving policy objectives, minimising the burden of regulation, and doing this as efficiently as possible.

There are a number of purposes for which guidance material may be prepared. These include assisting people to understand what the law says or requires, and providing up-to-date technical advice. Guidance material can be used to deal with emerging issues at the national and jurisdictional level for which a regulatory response is either not appropriate or not yet developed.

Standards Australia also has the capacity, if and when appropriate, to advise Government on Australian Standards that could be mandated in legislation. An example of this is our technical committee on Electromagnetic Compatibility (EMC) TE3. Under the EMC arrangements, Standards Australia as the standards body, through the EMC committee, develops Australian EMC standards and provides Australian input to International EMC standards. The Australian Communication and Media Authority (ACMA) currently utilise this mechanism for their standard development requirements.

The availability of codes of practice is essential to the application of the telecommunications acts and related regulations by employers. Codes of practice are particularly important for guidance on technical issues where regulations may have traditionally provided little in the way of specific technical requirements.

The development of nationally-aligned codes of practice would seem to be a more efficient solution in terms of government resources, and would provide better clarity for industry. Australian Standards could play a valuable role as one form of code of practice, over and above their use as ‘guidance material’. The established Standards development process ensures that such documents are nationally consistent, allow equal access and are internationally aligned as appropriate to comply with WTO TBT requirements, that they have consensus support of the regulators who will apply them (and who have been involved in their development), and consensus support of the industries (employers and employees, who have again helped to develop the Standards) which will use them.

Australian Standards are also often used as alternatives to black-letter regulation or adopted in regulation that has a direct impact on information security management. They are drafted jointly by regulators and stakeholders to achieve good regulatory practice. For example, communications and broadcasting committees exist within Standards Australia. They comprise of experts in their field who can assist greatly in developing relevant standards for deploying the NBN. Such committees include:

- ISO JTC 1/SC 27 IT Security techniques (The international committee)
    - IT 12-04: Information Security Management (The Australian mirror committee)
- ISO TC 68: Financial Services (The international committee)
    - IT-005: Financial Transaction Systems (The Australian mirror committee)

Our international participation is integrated with national standardisation. This means that Australia, through Standards Australia, is involved as a participating member or observer in a number of ISO and IEC committees. For clarification, a participating member means that a member is required to vote on a committee for things like changes to standards, whereas an observer is just that and is ineligible to vote but has access to all pertinent materials.

<u>ISO JTC 1/SC 27</u>

JTC 1/SC 27 has 41 participating countries and 12 observer countries on its committee upon which Australia is a participating member. Participating membership means that we are ale to case vote on drafts and matters arising from the ISO forum in relation to this sub committee. We are also able to send delegations of experts to represent Australia at international standards meetings, where this is appropriate and funded. Standards Australia is currently developing international pathways which will give funding options to stakeholders.

JTC 1/SC 27 has 87 published ISO standards under its direct responsibility. The scope of this Committee includes Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.

Sub-committees and working groups for JTC 1/SC 27 include:

Subcommittee/Working Group	Title
JTC 1/SC 27/WG 1	Information security management systems
JTC 1/SC 27/WG 2	Cryptography and security mechanisms
JTC 1/SC 27/WG 3	Security evaluation criteria
JTC 1/SC 27/WG 4	Security controls and services
JTC 1/SC 27/WG 5	Identity management and privacy technologies

IT 012-04

Information Security Management System (ISMS) standards are relevant to any organisation reliant on information and IT such as large corporates, SME’s and Government agencies.

The ISMS standards specify a framework for organisations to manage information security aspects of their business and if necessary to demonstrate to other parties (for example, business partners, auditors, customers and suppliers) their ability to manage information security.

The 27000 Standards series

The rise in visibility of information security across the world has been recognised by the international committee. They have been engaged over the last several years in drawing together core information security and critical infrastructure standards into a coherent body of work. These standards are called the ‘27000 series’. All of these standards have a five digit identifier, namely 27 X X X (please refer to Appendix C).

ISO/IEC 27001 ‘Information Security management Systems – Requirements’’ is the foundation standard and it is applicable to all types of organisations and all sectors of the economy. It specifies a risk-based management system that is designed to ensure that organisations select and operate adequate and proportionate (i.e. cost effective) security controls to protect information assets. The standard also shows how requirements relate to the OECD Guidelines for the Security of Information Systems and Networks.

There are also generally applicable ISO/IEC and/or Australian/NZ Standards covering, to name several:

- Digital signatures;
- Encryption (algorithms, modes of operation, key management);
- Entity authentication;
- Hash functions;
- Intrusion detection;
- IT evidence collection;
- Message authentication codes;
- Network security;
- Non repudiation;
- Prime number generation;
- Random number generation;
- Security evaluation of products;
- Security incident management;
- Time-stamping; and
- Trusted third party services

ISO TC 68

TC 68 – Financial Services has 25 Participating Countries on its Committee along with 35 Observers upon which Australia is a participating member. It has 50 published ISO Standards relating to the TC and its Sub Committees. The scope of TC 68 is Standardisation in the field of banking, securities and other financial services.

Sub-committees and working groups for TC 68 include:

Subcommittee/Working Group	Title
TC 68/TG 3	Trade Services - Trade Finance SEG
TC 68/TG 5	Cards & Related Retail Financial Services
TC 68/TG 2	Securities - Securities SEG
TC 68/TG 1	Payment - Payment SEG
TC 68/CAG	Chairman's advisory group
TC 68/TG 6	Technical Support for ISO 20022
TC 68/TG 4	Foreign Exchange - "FX SEG"
TC 68/WG 4	Management of ISO 20022

TC 68/SC 2	Security management and general banking operations
TC 68/SC 4	Securities and related financial instruments
TC 68/SC 7	Core banking

IT-005

The prime function of IT-005 is standardisation in the area of electronic funds transfer and involvement in ISO work on this and related subjects.

Participation in the work of International Technical Committees, Subcommittees and Working Groups, includes ISO/TC 68 SC2 (Security Management and General Banking Operations), SC4 (Securities and Related Financial Instruments) and SC6 (Core Banking).

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

- ***Education initiatives***
- ***Legislative and regulatory initiatives***
- ***Cross-portfolio and inter-jurisdictional coordination***
- ***International co-operation.***

Standards Australia recognises that independent of the regulatory approach Governments decides to take when faced with policy issues, uniformity is required. This is especially true in the context of a national approach to information security management and cyber crime. Consistency is essential to enhance national productivity and assist in diminishing the regulatory burdens and associated costs for business.

Whatever system is used, harmonisation both nationally and internationally must be ensured and this is what national standards are designed to do. Australian Standards® directly answer the Committees concern for processes that mitigate e-security risks faced by Australian consumers and the Committee is a balanced, representative group of experts from:

- Government;
- Industry;
- Academia; and
- Consumer groups using a concessus-based process.

Moreover, nationally consistent Australian Standards allow for cross-portfolio and inter-jurisdictional coordination. This will allow for interoperability and communication of information and reporting.

Standards help make laws and regulations consistent across Australia. By using a Standard, a South Australian consumer law becomes consistent with a NSW fair trading regulation. Standards also offer an alternative to regulation, with less red tape and business costs, while still providing security for families and small business consumers.

Australian Standards have the additional benefit of being drafted jointly by regulators and technical experts in this space (stakeholders). For example, as the Australian member of the International Electrotechnical Commission, Standards Australia works very closely with energy regulators, unions, employers and other stakeholders in both Australia and New Zealand to harmonise electrical practice and mitigate risks of serious injury and death associated with electrocution. Under this system, jurisdictions have the prerogative to decide whether or not to mandate the standard into regulation.

Regulatory structures can be depicted as pyramids with legislation and regulation at the apex, supported by codes, with standards at the base. Australian Standards offer each sectoral regulatory ‘pyramid’ a sound and consistent base and can do the same to further address the needs of the information management sector.

Standards Australia: Our Business Model

Standards Australia has undertaken a significant business transformation to ensure its activities are sustainable and that it can continue to serve the Australian community through the delivery Australian Standards well into the future.

As noted in Appendix A, Standards Australia introduced a new business model in October 2008 to increase efficiency and focus its limited resources where they can deliver the most benefit to Australia on a prioritised, economy wide, sectoral and cross-sectoral basis. This business model emphasises that responsibility for identification of needs, solution and solution provider must be provided by the relevant community of interests. Where a Standard is selected from the continuum of regulatory and non-regulatory options, there are market choices in relation to niche and accredited Standards Development Organisations, including Standards Australia. For Standards Australia to evaluate and prioritise a proposal for an Australian Standard, demonstrated stakeholder commitment and up front agreement on sufficient resources and funding are required to ensure agreed, balanced, robust and timely outcomes.

It is the opinion of Standards Australia, based on the policy direction and potential work program of the Committee and DBCDE, that the most suitable choice for the development of accelerated standards to address key recommendations out of this inquiry would be the ‘collaborative pathway’.

This pathway is a customised solution which will provide flexibility and choice, acknowledging that stakeholders and the community will be in a position to contribute the resources and funding required to develop standards expeditiously.

As mentioned above, Standards Australia currently has a number of collaborative relationships and projects which include:

- Department of Heath and Ageing (DoHA) – Health Informatics (IT14);
- Department of Environment, Water, Heritage and the Arts (DEWHA) – Energy efficiency standards; and

- The South Australian Government – Environmental Protection Authority (EPA) – Greywater treatment for river vessels.
- Centrelink – Development of a new Australian Standard® for new smart card authentication of ID.

Standards Australia's business model was introduced following extensive stakeholder consultation conducted by Standards Australia. The business model also takes into account and aligns with recommendations put forward by the Productivity Commission in its 2006 review and report on Standard Setting and Laboratory Accreditation. These recommendations included that the development of Australian Standards be supported by the client government agency, for domestic standardisation activities (Recommendation 9.1 of the PC Report in November 2006).

Conclusion

Standards Australia supports the Government's initiative for ensuring the safety of information and privacy of the Australian community. Standards Australia has the expertise to assist in providing economic development that is sustainable and efficient through its expert technical committees and to meet national obligations and interests.

Standards Australia, as the nation's peak non-government standards development body, has a very important role to play in the development of Australian Standards. They are an important component of a harmonised regulatory approach.

Standards Australia would welcome increased engagement with DBCDE to maximise the benefits which may be gained from development and utilisation of relevant and effective Australian Standards in meeting the telecommunications challenges of the future.

Appendix A: Standards Australia

Standards Australia is recognised by the Commonwealth Government as the nation's peak Standards body. It is a not-for-profit, non-government organisation that coordinates standardisation activities and facilitates the development of Australian Standards® by working with Government, industry and the community.

Standards Australia also promotes excellence in design and innovation through the Australian International Design Awards.

Standards Australia responds to national needs for contemporary, internationally aligned Standards that deliver Net Benefit to Australia (i.e. the benefits must outweigh the costs – all Australia Standards must have a positive effect on relevant communities of interest) (Net Benefit) by:

- coordinating representation of Australian input into international standards development and adoption, promoting information exchange and knowledge management through our National Standards Office (NSO);
- accrediting Standards Development Organisations (SDOs) through the highly autonomous Accreditation Board for Standards Development Organisations (ABSDO); and
- developing internationally harmonised Australian Standards and other normative technical documents through expert Committees within Standards Australia Standards Development (SA SD) as a major ABSDO accredited SDO.

Standards Australia is Australia's member of the Pacific Area Standards Congress (PASC), International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Council of Societies of Industrial Design (ICSID), providing a direct link to the regional and international arena and creating further efficiencies. It offers support to Government in relation to such for a as the APEC Standards and Conformance Subcommittee (ASPEC SCSC) and to business through the APEC Business Advisory Council (ABAC).

Standards Australia has a catalogue of around 7,000 existing standards, which it maintains in order to ensure currency and order. Standards Australia's standards development activities are undertaken in compliance with the World Trade Organization Agreement on Technical Barriers to Trade. Standards Australia has over 450 active projects currently under development.

To support this work and assist the interface between non-government standards legislation and regulation, a Memorandum of Understanding (MoU) has existed between Standards Australia and the Commonwealth Government since 1988, as reviewed from time to time.

Australian Standards set specifications and guidelines to ensure the quality, safety, reliability and consistency of products and services, developed in accordance with ABSDO's Requirements for Accreditation of Standards Development Organisations and Criteria for Designation as an Australian Standard. These specify the effort required of consensus groups such as Technical Committees under the authority of an accredited SDO to achieve consensus and ensure the interests of all stakeholders are considered during the development of an Australian Standard.

In October 2008, Standards Australia Standards Development introduced a new business model to improve Standards development processes, enhance engagement with stakeholders, and provide stakeholders with choice in development pathways. The new business model allows Standards Australia Standards Development to focus its limited resources where they can deliver the most benefit to Australia, and will ensure its long-term financial sustainability in perpetuity.

This new business model was introduced following extensive stakeholder consultation conducted by Standards Australia. The new business model also takes into account and aligns with recommendations put forward by the Productivity Commission in its 2006 review and report on Standard Setting and Laboratory Accreditation. These recommendations included that the development of Australian Standards be funded by the client government agency, for domestic standardisation activities (Recommendation 9.1 of the PC Report in November 2006).

Standards Australia is a public company limited by guarantee. More than 70 of Australia’s leading industry, government and consumer organisations form the Members of the Standards Australia Council. The Council has the responsibility to elect the Board of Directors, the Accreditation Board for Standards Development Organisations (ABSDO) and to appoint new Members to the organisation. The Standards Australia Council is responsible for the general oversight of standardisation in Australia and the governance of Standards Australia.

Appendix B: What is an Australian Standard®?

Australian Standard® branded standards are developed by accredited Standards Development Organisations (including Standards Australia) in accordance with ABSDO's criteria and requirements [refer to www.absdo.org.au and www.standards.org.au (then follow HOME › AREAS & ACTIVITIES › COORDINATION & INFORMATION)]. These websites list a number of documents concerning the accreditation process, including:

- NSO Procedure 1: Standards Development Projects;
- Requirements for Accreditation of Standards Development Organisations;
- Criteria for Designation as an Australian Standard;
- Access to Australian and International Standards;
- Numbering of Australian Standards; and
- The Guide to Net Benefit.

The development of Australian Standards involves voluntary participation from relevant industry, government, community and other interested parties via balanced technical committees. Australian Standards are documents that are regularly reviewed to allow for research, changes and advancements in community expectations, technical, legal and environmental factors.

Australian Standards offer a mechanism for guidance with which compliance is not mandatory unless the Standard is incorporated into law by government.

The decision as to whether a Standard will become mandatory and given regulatory effect is usually indicated at the commencement of the Standards development process as a result of regulatory arrangements managed by various Commonwealth, State and Territory government bodies.

Standards are developed according to due process which provides them with their authority and widespread acceptance. That due process is centred on consensus, transparency, participation on a non-discriminatory basis and impartiality.

The Standards development process within Standards Australia Standards Development involves the following steps:

- Request for development of a new Australian Standard;
- Evaluation on national needs, costs and benefits;
- Approval of new Standards development project;
- Committee formed;
- Committee develops draft;
- Public comment on draft;
- Consideration of comments;
- Ballot; and
- Publication.

Appendix C: Sample National and International Standards Relating to Information Security

Number	Publication Title	Designation	Year
1.	Health informatics - Information security management in health using ISO/IEC 27002	ISO 27799-2008	2008
2.	Information technology - Security techniques - Code of practice for information security management	AS NZS ISO IEC 17799-2006 AMDT 1	2008
3.	Information technology - Security techniques - Information security risk management	ISO IEC 27005-2008	2008
4.	Information technology - Security techniques - Code of practice for information security management - Technical Corrigendum 1	ISO IEC 17799-2005 COR 1-2007	2007
5.	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	ISO IEC 27006-2007	2007
6.	Information technology - Security techniques - Code of practice for information security management	AS NZS ISO EC 27002-2006	2006
7.	Information technology - Security techniques - Code of practice for information security management	AS NZS ISO IEC 27002-2006	2006
8.	Information technology - Security techniques - Information security incident management	AS NZS ISO IEC 18044-2006	2006
9.	Information technology - Security techniques - Information security management systems - Requirements	AS NZS ISO IEC 27001-2006	2006
10.	Financial services - Information security guidelines	ISO TR 13569-2005	2005
11.	Information technology - Security techniques - Code of practice for information security management	ISO IEC 17799-2005	2005
12.	Information technology - Security techniques - Code of practice for information security management	ISO IEC 27002-2005	2005
13.	Information technology - Security techniques - Information security management systems - Requirements	ISO IEC 27001-2005	2005
14.	Information security - Code of practice for information security management	AS NZS ISO IEC 17799-2001 AMDT 1	2004
15.	Information security risk management guidelines	HB 231-2004	2004
16.	Information technology - Code of practice for information security management	AS NZS ISO IEC 17799-2001 AMDT 1-2004	2004
17.	Information technology - Security techniques - Information security incident management	ISO IEC TR 18044-2004	2004

18.	Information security management - Implementation guide for the health sector	HB 174-2003	2003
19.	Information security management - Specification for information security management systems	AS NZS 7799.2-2003	2003