SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
ATTORNEY-GENERAL'S DEPARTMENT

Output 2.2

Question No. 73

Senator Ludwig asked the following questions at the hearing on 31 October 2005:

GovCERT and the Information Technology Security Expert Advisory Group (ITSEAG)

a) Could you identify the members of the government program that are currently on the information technology security expert advisory group?
b) Is GovCERT on this team?
(i) If not, why not? If so, what are its functions on the team? And, when did it join the team?
c) Could you indicate how many members of the team left this year, and when they left?
d) Were reasons sought as to their departure?
(i) If not, why not? If so, what were the reasons?
e) What reasons did AusCERT give for leaving the team?
f) Has the Department since approached AusCERT about rejoining the team?
g) Have any new members joined?
(i) If so, who has joined?
(ii) If not, have you sought any to replace the outgoing members of the team?
(iii) If so, what has their response been?
h) What are the terms of reference the team operates under?
(i) Does it produce reports, or analysis?
(ii) If so, what sorts of reports and analysis does it produce?
(iii) How does it set its priorities, and to whom does it disseminate them?
i) Does the body initiate programs of its own accord; is it responsible for running programs?
(i) If not, why not? If so, what programs has it initiated within the reporting period?

The answers to the honourable senator's questions are as follows:

a) The Department of Communications, Information Technology and the Arts (DCITA) chairs the IT Security Expert Advisory Group (ITSEAG) which has the following members:

- Queensland University of Technology (Professor William Caelli)
- Australian Research Council (Professor Ah Chung Tsoi)
- Symantec (Mr Tim Hartman)
- Internet Security Systems (Mr Kim Duffy)
- Microsoft Australia (Mr Greg Stone)
- Defence Signals Directorate (Ms Carolyn Patteson)
- GovCERT (Mr David Campbell)
- Defence Science and Technology Organisation (Dr Mark Anderson)
- Tenix Pty Ltd (Mr Geoff Rhodes) as a nominee of the Australian IT Security Forum
- National Information Communications Technology Australia (Mr James Galloway)

b) Yes, GovCERT is a member of the ITSEAG.

(i) GovCERT joined the ITSEAG in June 2005. GovCERT, as a desk within the Attorney General's Department, is responsible for planning government response to major Internet security incidents. Its function within the ITSEAG is to draw on its expertise and networks to provide guidance on IT security issues as they relate to critical infrastructure protection.

c) Members who have left the ITSEAG are:

- Mr Graham Ingram, AusCERT – March 2005
- Mr Troy Braban, eB2B com – March 2005
- Mr David Jonas, Convergence e-Business – March 2005
- Mr Peter Penfold, Compucat Research – March 2005. Mr Penfold was a nominee of the Australian IT Security Forum (an operating forum of the Australian Electrical and Electronic Manufacturers' Association (AEEMA).
- Mr John Donovan, Symantec –September 2005. Symantec continues to be represented on the ITSEAG. Mr Tim Hartman replaced Mr Donovan on the Group.
- Mr Neil Bryans, Defence Science and Technology Organisation (DSTO) – March 2005. DSTO continues to be represented on the group with Dr Mark Anderson as the new representative.
- Mr Steven Stroud, GovCERT – November 2005. Mr Steven Stroud was the first representative of GovCERT on the ITSEAG who joined the group as a GovCERT representative in March 2005. Mr David Campbell took-over the GovCERT responsibilities from Mr Stroud in early November and as a result he is now the GovCERT representative on the ITSEAG.

d) No, some members left on the expiry of their term, others left due to changes in their organisation or priorities.

(i) According to the Terms of Reference, ITSEAG membership is for a period of one year with the possibility of a one-year extension at the discretion of the Trusted Information Sharing Network's (TISN's) peak body the Critical Infrastructure Advisory Council (CIAC). At the expiry of their first term, the Chair had informal discussions with members about their future involvement with the group with a view to maintaining a broad base of expertise and knowledge relevant to the forward work program. The preference to maintain some continuity in the membership of the group was also a factor.

e) As the membership of the group was under consideration for its second year, Mr Ingram, General Manager, AusCERT advised the Chair that AusCERT would not seek to continue its representation. Mr Ingram confirmed this at the ITSEAG meeting in March 2006.

f) Membership of the ITSEAG is reviewed annually. The current membership will continue until early next year at which time appointment of new members will be considered.

g) Yes.

(i) New members of the ITSEAG are:

- Mr Greg Stone, Microsoft Australia (Joined April 2005)
- Mr James Galloway, National Information Communications Technology Australia (NICTA) (Joined April 2005)
- Mr Andy Solterbeck, Senetas Corporation Limited as a nominee of the Australian IT Security Forum (Joined April 2005 and left September 2005)

- Mr Geoff Rhodes, Tenix Pty Ltd as a nominee of the Australian IT Security Forum (Joined September 2005)
- Dr Mark Anderson, DSTO (Joined April 2005)
- Mr David Campbell, GovCERT (Joined November 2005)

(ii) Not applicable

(iii) Not applicable

h) The Terms of Reference for the ITSEAG are as follows:

Information Technology Security Expert Advisory Group

(ITSEAG)

Terms of Reference

Statement of Key Principles

The Australian community, the economy and the delivery of government services are all dependent upon the provision of robust and resilient infrastructure. The private sector owns or operates the majority of Australia's infrastructure including that which is determined to be critical to the national interest. As a matter of good governance, the corporations that own or operate critical infrastructure have the primary responsibility for addressing the security of their assets. In order to make informed decisions to invest in risk mitigation the owners and operators of critical infrastructure require current and relevant information on generic threats and vulnerabilities in their industry sectors and an understanding of the risks posed to them by their own dependence on other critical infrastructure.

Critical infrastructure protection (CIP) requires a national approach and a cooperative partnership to ensure consistency between the Commonwealth, the States and Territories, and the owners and operators of critical infrastructure. To enable the sharing of generic security threat and vulnerability information between corporations and between government and the private sector, the Australian Government has created the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). Although other fora exist to discuss IP issues, the TISN provides a mechanism to share information on the medium to long-term aspects of CIP, particularly relating to the national interest, cross-sector interdependencies, regulatory impediments and research.

The activities of this group should be in accordance with the principles contained in the National Strategy for Critical Infrastructure Protection.

Definition & Purpose

1. The Information Technology Security Expert Advisory Group (ITSEAG) forms part of the TISN.
2. The TISN comprises the Critical Infrastructure Advisory Council (CIAC), sectoral Infrastructure Assurance Advisory Groups (IAAGs) and Expert Advisory Groups (EAGs). It has been created in the national interest and is intended to facilitate the owners and operators of critical infrastructure sharing information on important issues relating to generic threats to, and vulnerabilities in, critical infrastructure and appropriate measures and strategies to mitigate risk.
3. Due to the increasing interconnectedness of business sectors in a modern economy, all CI sectors are likely to confront some common, cyber-related issues.

It is recognised that a broad Information Technology (IT) security perspective is required to inform the decision-making and planning of all bodies represented within the TISN.
4. The ITSEAG will provide information and guidance to the CIAC on technical solutions to problems identified by the sectoral groups, and provides the CIAC with a projection of emerging or future IT security trends that have the potential to impact on all industry sectors. It will also assist in the review of CIP research proposals and provide suggestions to the CIAC on specific CIP research and development projects.
5. The ITSEAG will report directly to the CIAC, which may provide directions for its operations or refer specific issues for its consideration. The IAAGs may also refer specific items to the ITSEAG. Subject to the above and to the CIAC's overseeing role referred to at paragraph 9, the ITS EAG can set its own priorities.
6. The ITSEAG will not provide incident response support to the TISN. Nor is it the role of the ITSEAG to provide specific detailed advice to the TISN on technical solutions identified by CI owners and operators.

Critical Infrastructure
7. Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security.

Relationship to CIAC
8. The responsibility for the interpretation of, or alteration to, these terms of reference rests with the CIAC. The CIAC is charged with maintaining good governance of the TISN and to that end will provide oversight of the ITSEAG as detailed in these Terms of Reference.
9. The CIAC also forms part of TISN, and consists of representatives of each critical infrastructure sector, a representative of each of the States and Territories, and representatives of relevant Australian Government agencies. The CIAC will advise the Attorney-General on matters of nationally significant CIP. The CIAC will also report to the National Counter-Terrorism Committee as appropriate on matters concerned with nationally significant CIP. Matters regarding major issues of national significance with respect to CIP or those involving cross-sectoral interdependencies should be referred to the CIAC for consideration.

Scope of these Terms of Reference
10. These Terms of Reference cover the operation of the Information Technology Security Expert Advisory Group. Each Expert Advisory Group and sectoral Infrastructure Assurance Advisory Group has separate Terms of Reference, as does the CIAC. The Terms of Reference are required to ensure that information sharing under the auspices of the TISN is not used to carry out activities that might be in conflict with obligations that exist for individuals and corporations under any legislative or regulatory regimes.
11. Adherence to these Terms of Reference is a condition of membership of the ITSEAG.

Permissible Discussions
12. The ITSEAG has been formed to facilitate the consideration of IT security issues in relation to CIP across the TISN. The discussions may include (but are not limited to) the following:
- The dependence on IT within critical infrastructure;

- Vulnerabilities in and threats to IT systems supporting critical infrastructure;
- The efficacy of risk mitigation strategies for IT systems, threats or vulnerabilities; and
- The available IT security resources within Australia, including skills, products, services and research.

13. The ITSEAG will not generally be used as the forum for the discussion or communication of nationally classified threat assessment information or levels of threat. Sector specific threat assessments or environmental assessments aimed at protective security planning will be communicated to the industries concerned by an appropriate Australian Government agency, State or Territory police, or in conjunction with each other. Threat assessment information of a specific or immediate nature will be communicated by State or Territory police to affected industry parties under existing National Counter-Terrorism arrangements.

14. Participants shall not use the ITSEAG as a forum for marketing products or technology but shall operate in a vendor-neutral manner.

15. The sharing of information must not be in contravention of, or conflict with, any legal obligations. This includes obligations under the *Trade Practices Act 1974* and the *Corporations Act 2001*.

Participants shall maintain an awareness of the provisions contained in Part IV of the *Trade Practices Act* which prohibits certain types of anti-competitive conduct. Participants shall not use the forum to engage in any activity or conduct that is in breach of the *Trade Practices Act*.

16. Discussions involving personal information shall be held in accordance with obligations under the *Privacy Act* 1988 (Cth) or any other law in relation to privacy or protection of personal information as amended from time to time.

Membership

Principle of Membership

17. The ITSEAG will comprise academic specialists, representatives from IT security companies, and consultants who are selected for their individual expertise rather than as representatives of their organisations.

Administrative Arrangements

18. The Department of Communications, Information Technology and the Arts (DCITA) will coordinate nominations for ITSEAG membership, which will be put to the CIAC for endorsement.

19. Members will be appointed for one year with the possibility of a one year extension at the discretion of the CIAC where continuity of consideration of issues is necessary.

20. The ITSEAG will normally have no more than ten members, although temporary members may be added on an ad hoc basis to deal with specific issues.

21. A breach of these terms may result in the termination of a participant’s membership. Any alleged breaches of these terms or of the principle of membership, or issues of membership termination, shall be referred to CIAC for determination.

Reporting

22. The ITSEAG shall submit an annual report regarding its activities to the CIAC in line with its anticipated meeting schedule.

23. As appropriate, the ITSEAG may submit reports to CIAC and the IAAGs providing information and guidance on IT security matters.

Communications

24. All public statements to be made on IT security issues and on behalf of the TISN as a whole shall be made by the CIAC.

Internal Administrative Arrangements

25. Secretariat support to the ITSEAG will be provided by DCITA.
26. The Chair of the ITSEAG will be nominated by DCITA in consultation with the ITSEAG members.
27. The ITSEAG may establish working arrangements, such as the use of working groups and sub-committees that will best allow it to carry out its functions.
28. In addressing specific issues, it is expected that the ITSEAG will work closely with sector-based IAAGs to ensure that the ITSEAG is aware of the needs of the IAAGs and is able to tailor its information and guidance to meet these needs. This may be done through joint meetings, workshops, surveys and other methods as appropriate.
29. Other internal administrative procedures, including the frequency of meetings and the length of appointment of chairs, shall be determined by the ITSEAG.

Deed of Confidentiality

30. All members or the ITS EAG shall agree to adhere to the TISN Deed of Confidentiality where it is likely that confidential information will be the subject of discussion or presentation or included in written material to be submitted to the group.
31. Where a breach of the Deed of Confidentiality is alleged, the issue shall be referred to the CIAC.
32. Where individuals or organisations are involved in the ITS EAG on an *ad hoc* or temporary basis, they are only required to sign the Deed of Confidentiality where it is likely that confidential information will be the subject of discussion or presentation or included in written material to be submitted to the group. The ITSEAG shall determine appropriate arrangements in these circumstances.
33. Representatives of the Crown may be requested to sign the Government Representative Confidentiality Acknowledgement Form where confidential information will be the subject of discussion or presentation or included in written material submitted to the group. Representatives of the Crown are not required to sign the Deed of Confidentiality due to existing legal obligations that provide for confidentiality.

(i) The ITSEAG provides guidance on IT security issues throughout the TISN. This guidance can be in the form of reports, papers or workshops.

The ITSEAG reports regularly to the peak body of the TISN, the Critical Infrastructure Advisory Council (CIAC), on its achievements and overview of its forward work program.

(ii) The ITSEAG has produced papers targeted at senior management of critical infrastructure organisations on a number of strategic e-security issues identified by the membership. These have included to date:

- Security of wireless applications
- Security aspects of Voice over Internet Protocol and
- Supervisory Control and Data Acquisition (SCADA) systems Security.

These are available on the TISN website: www.tisn.gov.au

(iii) The priorities of the ITSEAG are set by the CIAC.

i) The ITSEAG does not initiate or run programs.

(i) The ITSEAG was not established to initiate or run programs. Rather, it provides guidance to CIAC and critical infrastructure owners and operators within the TISN on IT security in the form of advisories and other awareness raising initiatives such as workshops.