

Australian Voluntary Code of Conduct for ISPs – Rohan Buettel

A recommendation of the 2008 E-security Review was that the Australian Government work with ISPs to develop a Cyber Security Code of Practice. The preferred mechanism is for an industry developed, voluntary code. The Internet Industry Association (IIA) of Australia is leading the development of the Code. The Australian Government provided the IIA with funding totalling \$30,000 to scope issues for the Code and develop a suitable consultation process involving ISPs, consumer groups and other relevant stakeholders.

The proposed voluntary ISP code of conduct has three broad aims:

- To empower Australians to be responsible for their internet security;
- To encourage and perhaps formalise information sharing amongst ISPs in relation to cyber security threats and attacks; and
- To formalise and standardise remediation steps for ISPs and their customers where customer's computers have become infected with malicious software.

There are two aspects to the problem that the code is designed to address: detection of infection and remediation of infected computers. The draft code suggests ISPs make use of ACMA's Australian Internet Security Initiative (AISI); that they could use information gathered through monitoring network health as part of normal network management (such as employing their existing anti-virus, intrusion detection or anti-spam capabilities); or they could access reporting from international anti-spam and online security experts.

One of the practical outcomes of the Code is that it will provide a standard approach for dealing with the notifications from ACMA, informing customers and assisting them in clearing their computers of malicious software.