



Australian Government

**Department of Broadband,
Communications and the Digital Economy**

Mr Rod Beckstrom
CEO and President
Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way
Suite 330
Marina Del Ray, CA 90292
USA

Dear Mr Beckstrom,

Response to questions about national Computer Emergency Response Teams (CERT)

Thank you for your questions of 21 April 2010, conveyed through former Governmental Advisory Committee Chair Janis Karklins, seeking information on the CERTs operating in Australia. Please see attached responses to your specific questions.

By way of general comment, Australia acknowledges the importance of a strong Domain Name System (DNS) and welcomes the continued efforts in the internet community to improve the security, stability and resiliency of the DNS.

The Department of Broadband, Communications and the Digital Economy has consulted with relevant Australian Government security agencies in preparing this response. These agencies have advised that if ICANN's proposed DNS-CERT is progressed, it will be critical that this new body collaborate and co-ordinate with national CERTs and existing technical capabilities that reside within the private sector internationally. If the proposal is progressed, CERT Australia has noted that it would look forward to working with DNS-CERT on cyber security issues affecting DNS infrastructure.

We would be happy to provide additional details on the CERT arrangements in Australia if required.

Yours sincerely

A handwritten signature in black ink, appearing to read 'P. Nettlefold', written over a faint circular stamp.

Peter Nettlefold
Director
Internet Governance, IPND, and Numbering Team
Department of Broadband, Communications and the Digital Economy
AUSTRALIA

2 July 2010

Responses to specific questions on Australia's CERTs:

1) What CERTs exist in Australia?

CERT Australia is Australia's national computer emergency response team and is managed by the Australian Government Attorney-General's Department. CERT Australia works to ensure that all Australians and Australian businesses have access to information on how to better protect their information technology environment from cyber based threats and vulnerabilities. CERT Australia is the initial point of contact for cyber security incidents impacting upon Australian networks and for international CERTs and foreign governments.

For more information see: <http://www.cert.gov.au/>

In addition, there are a number of private sector CERTs in Australia, including those based in specific companies.

Of particular note is AusCERT, which prior to the establishment of CERT Australia, performed many of the functions of Australia's national CERT. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia.

2) Are these CERTs mature and stable in size and function or still under development?

CERT Australia commenced initial operations in January 2010. It is a continuation and expansion of the services previously provided by the Australian Government Computer Emergency Readiness Team (GovCERT.au), which provided information and assistance to the owners and operators of Australia's critical infrastructure and key business. This work continues under CERT Australia and represents a mature and stable function. CERT Australia continues to enhance its operational capability throughout 2010.

3) Are there any new CERTs under consideration in Australia?

Only to the extent that specific companies in the private sector may establish similar functions. CERT Australia is Australia's national CERT and there is no intention to alter these arrangements.

4) Are there any DNS or Botnet experts at the Australian CERTs that might be interested in joining a future possible network of experts on the topics. If so, please share any names and contact information as appropriate.

CERT Australia staff possess a range of expertise. This includes expertise in infrastructure (including DNS) and botnets. CERT Australia would be happy to consider participation in future networks on these topics when the details of the commitment required and structure of these networks became available. CERT Australia can be contacted on info@cert.gov.au.