



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

# FACT SHEET

## Computer Network Vulnerability Assessment Program

The Computer Network Vulnerability Assessment (CNVA) Program is an Australian Government grants scheme developed to help secure critical infrastructure. It is managed by GovCERT.au—the Australian Government Computer Emergency Readiness Team, located in the Australian Government Attorney-General's Department.

The program provides dollar for dollar funding to help owners and operators of critical infrastructure to:

- identify major vulnerabilities within ICT systems, dependencies between networks, and to test the ability of systems to resist exploitation
- examine the security implications of planned changes to an information technology infrastructure, and
- assess associated physical and personnel security issues.

### Participation in the CNVA Program

The CNVA Program supports critical infrastructure owned and/or operated by the private sector and by government business enterprises.

The program seeks to ensure that there are adequate levels of protective security on critical infrastructure systems and networks, minimum single points of failure and tested recovery arrangements.

CNVA projects must relate to the identification of vulnerabilities and dependencies in ICT systems and networks associated with critical infrastructure. These networks could include for example, CCTV systems, SCADA systems and remote access solutions. Assessments must include threat identification, vulnerability identification, consequence analysis, risk assessment and prioritisation, testing, and the identification of protective measures.

The CNVA Program does not provide funding to fix vulnerabilities. However, the scoping of possible corrective action and a review of remediation measures can be incorporated into a CNVA project.



### Why undertake a CNVA Project?

Participating in the CNVA Program allows critical infrastructure owners and operators to undertake an independent third party security review of their ICT systems and networks. Participants obtain a report that identifies vulnerabilities and suggests possible remediation measures that will enable their organisation to demonstrate industry best practice in IT security, and improve business resilience.

### Confidentiality

The confidentiality of a participant's sensitive information is of paramount importance to the Australian Government and to the integrity of the CNVA Program. All information shared with the government under the program is treated in strict accordance with Australian Government security requirements. This ensures that organisations can participate without risk of unauthorised disclosure of sensitive or Commercial-in-Confidence information.

### How to apply

Applications forms can be downloaded from the TISN website ([www.tisn.gov.au](http://www.tisn.gov.au)) under the CIP Projects or National Information Infrastructure tabs. For further information email [cnva@ag.gov.au](mailto:cnva@ag.gov.au).

CNVA Program staff are available to discuss projects with potential applicants and to assist with the development of applications.

The eighth round of applications under the CNVA Program closes on **30 April 2008**. Applications can be lodged at any time prior to this date, although late applications will be accepted at the Attorney-General's Department's discretion.