THE federal Government has allocated more than $50 million over four years to safeguard critical infrastructure in Australia such as electricity grids, data centres and telecommunications networks.

Measures in the Critical Information Protection strategy include $5.5 million in funding to the Department of Communications IT and the Arts (DCITA) for the development of information sharing networks that allow for public and private sector organisations to securely exchange information on perceived threats within their industry sectors.

The funding is a part of the government's overall 'homeland security' style anti-terrorism readiness programs.

The so-called Trusted Information Sharing Network (TISN) lets the owners and operators of critical infrastructure - whether government or private sector - share information and strategies on issues including business continuity, consequence management, information system vulnerabilities and attacks from threats like worms and viruses, as well as e-crime and the protection of key sites.

The department said funding would be used to help telecommunications companies, internet service providers and broadcasting firms to improve overall infrastructure protection through co-operation and information sharing.

The DCITA funding will provide secretariat and other support for the Communications Sector Infrastructure Assurance Advisory Group (CSIAAG), that brings together the owner-operators and the communications sector into a confidential, 'trusted' environment.

It also aims to promote Critical Infrastructure Protection as an issue in the communications industry by contributing to the Critical Infrastructure advisory Council (CIAC) and the National Counter Terrorism Committee.

Funding will also support a new Information Technology Security Experts Advisory Group to advise the CIAC on network security aspects of infrastructure protection. It will also support computer network vulnerability testing activities within Australia's information infrastructure sector where e-security defences can be tested in a controlled environment.

Treasurer Peter Costello's ninth budget also committed a further $9.7 million in the next financial year toward developing biometric technologies aimed at controlling identity fraud at borders.

The funding includes $3.1 million to the Customs department to extend trials of its SmartGate facial recognition system to a second international airport and to additional users during the 2004-05 year. The present SmartGate trial is being conducted at Sydney Airport.

The budget also allocated $2.2 million to the Department of Foreign Affairs and Trade (DFAT) to test its prototype biometric passport to ensure its compatibility with US border control equipment. The US has mandated that all visa-exempt nations - which includes Australia, NZ and most European Union countries - must use biometric passports for entry by October 2006.

DFAT has already been funded to the tune of $6.5 million in the previous two budgets. The money was spent on assessing various biometric systems before settling on facial recognition as most suitable for use in passports.

The Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) was allocated $4.4 million to examine the use of biometric technologies in Australia's existing electronic visa and entry arrangements.

In 2004-05, DIMIA will also develop the capacity to store and use digital biometric images to identify clients each time they deal with the department. DIMIA said that by strengthening its ability to identify non-citizens through biometric technology, it could better combat the use of false identities.

The government said the measures would make it more difficult for terrorist and criminals to steal the identity of Australians travelling overseas, or travel to Australia under a false identity. It said identity fraud in Australia costs the community about $1.1 billion annually.