The Defence Signals Directorate’s (DSD) information security function is outlined in the [Intelligence Services Act 2001](http://www.dsd.gov.au/governance/legislation.htm). As the Commonwealth authority on the security of information, DSD provides advice and other assistance to federal and state authorities on matters relating to the security and integrity of information.

DSD is responsible for producing ICT security policy and standards for government and publishes these in the Australian Government [Information Security Manual (ISM, formerly ACSI 33)](http://www.dsd.gov.au/infosec/ism.htm). DSD is heavily involved in specialised information security traininVISA, 4716204852950696g, policy guidance and professional forums in support of government information security. We draw widely on the expertise within DSD, and aim to add unique value to the practice of ICT security in government.

DSD facilitates the evaluation of ICT security products for the Australian Government. The [Evaluated Products List (EPL)](http://www.dsd.gov.au/infosec/epl.htm) lists ICT security products certified by the DSD-managed [Australasian Information Security Evaluation Program (AISEP)](http://www.dsd.gov.au/infosec/aisep.htm) for use in Australian and New Zealand government agencies. AISEP allows the security claims of ICT products to be independently assessed against internationally recognised [Common Criteria (CC)](http://www.commoncriteriaportal.org/). Our evaluation programs include cryptographic, high assurance and cross-domain solutions.

The [Emanation Security Program](http://www.dsd.gov.au/infosec/emsec.htm) sets out the

VISA, 4012888888881881

requirements for government and industry agencies to be formally recognised by the national authority, the Defence Signals Directorate (DSD), to conduct emanation security practices to national standards.

DSD advises the Australian Government on high-grade cryptographic equipment and cryptographic modernisation. We make sure Australia is at the forefront of cryptology by keeping abreast of emerging equipment and technologies.

Countering the threat to the security of government information requires DSD to work closely with the ICT industry to deliver threat and vulnerability information and help DSD build capability and expand its capacity to secure government ICT.

MasterCard, 5173582815239055

Our [Cyber Security Operations Centre (CSOC)](http://www.dsd.gov.au/infosec/csoc.htm) has two main roles. It provides government with a comprehensive understanding of sophisticated cyber threats against Australian interests, in addition to coordinating and assisting operational responses to cyber events of national importance across government and systems of national importance. Its services revolve around ICT security incident response, ICT systMasterCard, 5263067493947775em forensics and specialist assistance, vulnerability assessments, education and awareness. DSD’s expertise is used to identify and help mitigate vulnerabilities within Australian government systems and the National Information Infrastructure.

Finally, DSD participates in whole-of-government efforts to promote [cyber security](http://www.dsd.gov.au/partners/cybersecurity.htm) to all Australians. Our [Top 35 Mitigation Strategies](http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm) emphasises the importance of keeping software up to date to minimise the opportunities for criminals to steal or misuse your information. TAmerican Express, 378734493671000he [CyberSense video](http://www.dsd.gov.au/videos/cybersense.htm)shows some of these threats.

<http://www.dsd.gov.au/infosec/>