Channels assigned for regional digital television repeater services and remote area commercial digital television services

ACMA has allotted and assigned digital channels for television repeater services in regional New South Wales, Queensland and Tasmania, and for commercial television services in remote central and eastern Australia, and remote and regional Western Australia. In each area, ACMA has also identified unassigned digital channels that may be used for other purposes.

The regions covered by the variations to the digital channel plans include inland and north coast New South Wales, central Queensland and north-east and west Tasmania.

The areas in remote central and eastern Australia where channels have been assigned are Mount Isa, Alice Springs and Katherine. The areas in remote and regional Western Australia are Albany, Broome, Carnarvon, Central Agricultural,

Esperance, Geraldton, Kalgoorlie, Karratha, Manjimup, Narrogin, Northam, Port Hedland, Roebourne, Southern Agricultural and Wagin. ACMA has also identified one additional channel in each of these remote areas to be reserved for a possible third commercial television service to operate in digital mode only.

In making these decisions, ACMA aims to achieve spectrum efficiency and to minimise changes to existing reception equipment for viewers to receive digital broadcasts. The desirability of broadcasters being able to use their existing infrastructure to broadcast their digital television services is also taken into account.

The plans may have some impact on the use of VCRs and set-top boxes, but only relatively minor disruption to viewers is expected. In most cases,

retuning of television sets and VCRs will be all that is required. Public information and education campaigns will provide advice for viewers on how to retune devices and alternative connection methods before any changes take place.

ACMA was required to formulate legislative schemes for the conversion of commercial and national television broadcasting services from analog to digital mode. Under these schemes, ACMA can develop and vary digital channel plans for areas throughout Australia.

The plans determine which channels are to be allotted to each licensee for the purposes of transmitting services in digital mode and the technical characteristics of those channels. In developing and varying digital channel plans, ACMA aims to plan channel allotments to

enable broadcasters to plan their digital transmission coverage to achieve the same level of coverage as with its analog coverage.

The decisions are contained in explanatory papers and variations to the commercial and national digital channel plans.

The papers and variations to digital channel plans for Inland and North Coast New South Wales, Regional Queensland (Central Queensland) and Tasmania, and commercial digital channel plans for Remote Central and Eastern Australia and Remote Western Australia are on the ACMA website at www.acma.gov.au (go to About ACMA: Publications & research > Broadcasting publications > Planning > Final digital channel plans (DCPs)).

Online crime: are you protected?

The internet has become an essential business, social, entertainment and educational resource, but the increasing level of economic transactions conducted on it is making the internet the focus of criminal activities. ACMA publishes advice for consumer and business computer users to help them minimise the chances of becoming a victim of online criminals.

TIPS FOR PROTECTING COMPUTERS AND PERSONAL INFORMATION

1. Install anti-virus and other security software, such as anti-spyware and anti-spam software. Use and update this software regularly. Use an auto-update facility if this is available. Most virus software can be set to scan computers at a set time. Information about anti-virus software is available from the Internet Industry Association website at www.iia.net.au.

2. Regularly download and install the latest security patches for computer software, including web-browsers. Use automatic software security updates where possible.

3. Use a firewall and make sure it is turned on. Firewalls help prevent

unauthorised access to computers, as well as unauthorised communications from them. More information about the use of firewalls is on the Internet Industry Association website at www.iia.net.au.

4. Delete suspect emails immediately. Don't open these emails.

5. Don't click on links in suspect emails. Visiting websites through clicking on links in suspect emails may result in malware (malicious software) such as 'trojans' being downloaded. This is a commonly used and effective means of compromising computers.

6. Only open an attachment to an

email where the sender and the contents of the attachment are known. Suspect emails should be deleted immediately. If an attachment needs to be opened, it should be checked by anti-virus software before opening.

7. Don't download files or applications from suspect websites. The file or application could be malware. Malware may be falsely represented as e-security computer protection software.

8. Use long and random passwords for any application that provides access to personal identity information, including computer logon information. Don't use

dictionary words as a password. Ideally, the password should be eight or more characters in length. Change passwords regularly.

9. Use a limited permission account for browsing the web, creating documents, reading email and playing games. A limited permission account is one that does not have 'Administrator' status and can prevent malicious codes from being installed.

More information about computer security is on the ACMA website at www.acma.gov.au (go to For the public: Content & advertising > Spam – junk email & messages).