Communications Resilience Administration Industry Group (CRAIG)

Terms of Reference

The *Communications Resilience Administration Industry Group* (CRAIG) has been established to help those in and associated with the telecommunications sector to understand the telecommunications environment and the specific systems, networks and assets within the sector that are essential to the continuity of the sectors' services, to identify the risk, vulnerabilities, and resilience challenges that affect the telecommunications sector, and to facilitate greater collaboration in the repair and recovery effort following a disaster/emergency.

The CRAIG is not seeking to duplicate work currently being performed by other groups such as the Trusted Information Sharing Network (TISN), but rather to provide the necessary operational support activities associated with the TISN Communications Sector Group (CSG) activity associated with ensuring critical infrastructure resilience in the telecommunications sector.

The CRAIG will meet and operate under two functional arrangements.

Function 1 - the CRAIG is to meet regularly to:

1. identify and create an access-protected Communications Alliance (CA) list of all relevant Operations Centre contact details and escalation points for use by Carrier Operations Centres to discuss and coordinate mutually agreed assistance;
2. define what is a disaster, or an emergency, that would trigger action by this group under its second function and set out the terms of support arrangements that may be available to recover from a disaster, or emergency and determine what is strictly a matter for suppliers to resolve themselves;

   Note: The intent is not to provide back-up capability where a supplier has not taken sufficient care to have redundancy arrangements (e.g. failure of a single cell site in an area where coverage can be accommodated by surrounding cell sites is not an emergency, however, a single cell site in a rural area may be an emergency where there is no other readily available coverage, or where the recovery time is greater than a specified timeframe. Failure of a supplier to have diverse back up paths and failure of a single path is not an emergency, however, a failure of all available back up paths may be.)
3. identify and document current assistance capabilities between suppliers for all hazards (e.g. natural or man-made disasters, including cyber-attacks);
4. evaluate and identify opportunities for improving the resilience of Australia's critical communications infrastructure;
5. consider possible solutions to cope with disaster and seize opportunities, in times of crisis, change and adversity to ensure ongoing provision of telecommunications to the community;
6. identify critical infrastructure locations to share with TISN CSG for co-ordination with State/Territory based agencies responsible for protection of infrastructure and the energy sector to assist in the protection of telecommunications infrastructure and rapid recovery in the event of a disaster; and
7. identify any impacts which may arise in the resilience of infrastructure due to advancements in technology (e.g. virtual SIMs, IoT, etc.).

Function 2 -the CRAIG is to meet on an ad-hoc basis, (as the need arises), to:

1. co-ordinate any agreed operational arrangements associated with the recovery from disasters / emergencies – as per the definition agreed from point 2 above.

Primary deliverables

- Constitution and Terms of Reference;
- A contact list to be used during disasters to help resolve and recover from disaster;
- Operational arrangements for recovery from disasters/emergencies (e.g. cyber-attack).

"emergency" means a significant actual or imminent occurrence of an event, or events, which in any way endangers or threatens to endanger the ongoing ability to supply telecommunications services to the community.

Note: An emergency may arise as a result of, but not limited to, the following:

a. an earthquake, flood, wind-storm or other natural event;

b. a large-scale fire;

c. an explosion;

d. a plague or an epidemic or contamination;

e. a warlike act or act of terrorism, whether directed, or not, at the telecommunications industry, or customers of telecommunications services in Australia;

f. a hi-jack, siege or riot (e.g. action against a major telecommunications facility); or

g. large scale technological disruption to telecommunications services (e.g. such as might be caused by a Denial of Service cyber-attack).

Supporting deliverables

- Communications resilience strategy;
- Identification of what is considered critical infrastructure.