COMMUNICATIONS ALLIANCE LTD

INDUSTRY GUIDELINE

G663:2020

Telecommunications – Emergency Communications Protocol

G663:2020 Telecommunications – Emergency Communications Protocol Industry Guideline

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Industry Guideline:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Industry Guideline;

      ii) inaccuracy or inappropriateness of this Industry Code/Guideline; or

      iii) inconsistency of this Industry Guideline with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Code/Guideline.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

INTRODUCTORY STATEMENT

The Communications Alliance *Telecommunications – Emergency Communications Protocol (G663:2020)* has been developed to facilitate efficient interactions between the telecommunications industry and relevant Australian Government agencies when events cause major disruptions to telecommunications services.

The development of the Guideline was initiated in Q3 2019 by the Communications Resilience Administration Industry Group (CRAIG) within Communications Alliance, in preparation for the beginning of the 2019 bushfire season. Unfortunately, bushfires – and indeed a disastrous season – occurred earlier than expected and the work was placed on hold.

Following a Roundtable convened by the Hon. Paul Fletcher MP, Minister for Communications, Cyber Safety and the Arts, with telecommunications providers, regulators, consumer representatives and stakeholders from emergency organisations in January 2020, Communications Alliance committed to developing a Common Operating Model for telecommunications disaster management to underpin the efficient interaction between Australian Government agencies, telecommunications Carriers/CSPs (C/CSPs) and energy suppliers. Subsequently, the CRAIG resumed work on the Guideline.

This Guideline constitutes the Common Operating Model. More specifically, it is designed to:

(a) establish arrangements for pro-active engagement to mitigate the effects of a Major Service Disruption (MSD);

(b) set out competitively neutral and non-discriminatory approaches and processes;

(c) establish a common communications plan and streams for sharing of information between C/CSPs and between C/CSPs and energy suppliers;

(d) create awareness of evolving capabilities within the sector that may be used to support or complement each other during times of national level disasters and MSDs; and

(e) set out procedures between C/CSPs and Australian Government agencies, where communication procedures for MSDs do not already exist, to provide;

- guidance on the preferred means and processes for industry to report MSDs;
- a summary of the necessary details of an MSD to be shared in such circumstances;
- a common communications plan and streams for sharing of information between key industry stakeholders and Australian Government agencies; and
- processes to establish and maintain a key stakeholder contact list for use in MSDs.

Above all, during an MSD a C/CSP's priority lies with restoring and maintaining communications capabilities of its customers to the best of its abilities. As such, this Guideline is intended to be a simple and efficient way of facilitating adequate stakeholder and community communication without distracting staff from prioritised restoration duties.

Alexander R. Osborne
Chair
Communications Resilience Administration Industry Group

AUGUST 2020

TABLE OF CONTENTS

1	GENERAL	4
1.1	Introduction	4
1.2	Scope	5
1.3	Objectives	6
1.4	Guideline review	6
2	ACRONYMS, DEFINITIONS AND INTERPRETATIONS	7
2.1	Acronyms	7
2.2	Definitions	7
2.3	Interpretations	9
3	FACTORS INFLUENCING THE SEVERITY OF MAJOR SERVICE DISRUPTIONS	10
4	SEVERITY MATRIX	11
5	COMMUNICATIONS PLAN	13
5.1	Key Stakeholders	13
5.2	Major Service Disruption – Information Provision	14
5.3	Communication Principles	14
5.4	Contact List	15
6	MANAGING A MAJOR SERVICE DISRUPTION	16
6.1	Prevention	16
6.2	Preparation	16
6.3	Response	17
6.4	Recovery of Service	19
6.5	Reporting - Carrier and CSPs with wholesale channels	19
7	CYBER EVENT	20
8	HEALTH-RELATED EVENTS	20
9	REFERENCES	21
APPENDIX		22
A	CONTACT LISTS	22
B	PROTOCOL FOR NOTIFICATION OF MAJOR SERVICE DISRUPTIONS	23
C	CRISIS COORDINATION CENTRE	24
D	NOTIFICATION OF MAJOR SERVICE DISRUPTION	25

1 GENERAL

1.1 Introduction

1.1.1 Section 112 of the *Telecommunications Act 1997* (Act) sets out the intention of the Commonwealth Parliament that bodies and associations representing sections of the telecommunications industry develop industry codes relating to the telecommunications activities of participants in those sections of the industry.

1.1.2 The development of the Guideline has been facilitated by Communications Alliance through a Working Committee comprised of representatives from the telecommunications industry and Australian Government agencies.

1.1.3 The Guideline should be read in the context of other relevant codes, guidelines and documents, including the:

(a) *Protocol for notification of major service disruptions 2018;*

(b) *National Strategy for Disaster Resilience;*

(c) *Triple Zero Disruption Protocol 2020 (Ver 2.02);*

(d) Emergency Call Service Requirements Industry Code (C536:2011 Incorporating Amendment No.1/2015);

NOTE: In the case of disruptions to Triple Zero communications, the Triple Zero Disruption Protocol and industry code C536:2011 take precedence.

(e) *NSW State Emergency Management Plan;*

(f) *NSW Telecommunications Services Functional Area Supporting Plan*

(g) *Emergencies (Emergency Plan) 2014 (No1);*

(h) *Territory Emergency Plan;*

(i) *Queensland State Disaster Management Plan;*

(j) *State Emergency Management Plan (SA);*

(k) *Tasmania Emergency Management Plan;*

(l) *Emergency Management Manual Victoria;*

(m) *Western Australia Emergency Management Framework.*

1.1.4 The Guideline should be read in conjunction with related legislation, including the:

(a) Act;

(b) *Telecommunications (Emergency Call Service) Determination 2019*;

(c) *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)*;

(d) *Competition and Consumer Act 2010 (Cth);*

(e) *Privacy Act 1988 (Cth);*

(f) *Emergencies Act 2004 (ACT);*

(g) *Emergency Management Act 2013 (NT);*

(h) *Disaster Management Act 2003 (QLD);*

(i) *Emergency Management Act 2004 (SA);*

(j) *Emergency Management Act 2006 (TAS);*

(k) *Emergency Management Act 2013 (VIC);*

(l) *Emergency Management Act 2005 (WA);*

(m) *State Emergency and Rescue Management Act 1989 (NSW); and*

(n) *Essential Services Act 1988 (NSW).*

1.1.5 If there is a conflict between the requirements of this Guideline and any requirements imposed on a C/CSP, the other requirement or obligation takes precedence over this Guideline.

In particular, a C/CSP's contractual arrangements with its customers regarding Major Service Disruptions and other matters covered by this Guideline remain unaffected by this Guideline and have precedence over this Guideline.

1.1.6 Statements in boxed text are a guide to interpretation only.

1.2 Scope

1.2.1 The Guideline applies to:

(a) the Carriage Service Providers section of the telecommunications industry under section 110 of the Act and

(b) Australian Government agencies, and other sectoral bodies who choose to participate in the Guideline.

1.2.2 The Guideline deals with the following telecommunications activities as defined in section 109 of the Act:

(a) carrying on business as a Carrier; or

(b) carrying on business activities as a Carriage Service Provider; or

(c) supplying Goods or Service(s) for use in connection with the supply of a Listed Carriage Service.

1.3 Objectives

The objectives of the Guideline are to:

(a) establish arrangements for pro-active engagement to mitigate the effects of an MSD;

(b) set out competitively neutral and non-discriminatory approaches and processes;

(c) establish a common communications plan and streams for sharing of information between C/CSPs and between C/CSPs and energy suppliers;

(d) create awareness of evolving capabilities within the sector that may be used to support or complement each other during times of national level disasters and MSDs; and

(e) set out procedures between C/CSPs and Australian Government agencies, where communication procedures for MSDs do not already exist, to provide;

  (i) guidance on the preferred means and processes for industry to report MSDs;

  (ii) a summary of the necessary details of an MSD to be shared in such circumstances;

  (iii) a common communications plan and streams for sharing of information between key industry stakeholders and Australian Government agencies; and

  (iv) processes to establish and maintain a key stakeholder contact list for use in MSDs.

1.4 Guideline review

The Guideline will be reviewed 2 years after the Guideline's initial publication and every 5 years subsequently, or earlier in the event of significant developments that affect the Guideline or a chapter within the Guideline.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the Guideline:

ACSC

means Australian Cyber Security Centre

BCP

means Business Continuity Plan

CCC

means Crisis Coordination Centre

CSP

means Carriage Service Provider

DoS

means Denial of Service

DDoS

means Distributed Denial of Service

ECP

means Emergency Call Person

ECS

means Emergency Call Services

MSD

means Major Service Disruption

2.2 Definitions

For the purposes of the Guideline:

Act

means the *Telecommunications Act 1997 (Cth)*.

Carriage Service Provider

has the meaning given by section 87 of the Act.

Carrier

has the meaning given by section 7 of the Act.

Denial of Service

means a deliberate attempt to make access to the network unavailable to its intended users.

Department

means the Department of Infrastructure, Transport, Regional Development and Communications.

Distributed Denial of Service

means a deliberate attempt via multiple pathways to make access to the network unavailable to its intended users. The pathways can be from multiple sources within multiple Carriers, or multiple sources within a single Carrier.

Major Service Disruption

means a large-scale loss of connectivity from any point in a communications network that supports or delivers services to businesses and consumers.

NOTES: 1. For the purposes of the Guideline, an MSD is not related to a mass service disruption already provided for in legislation e.g. mass service disruption under the Telecommunications (Customer Service Guarantee) Standard 2011.

2. An MSD may occur due to inclement weather, natural or man-made disasters, equipment failure or other factors beyond a service provider's control. Refer to section 3 Severity Matrix for further factors.

Considerations of MSDs which may be reported, but are not limited to include MSDs which are:

- *Unexpected, non-scheduled outages unable to be resolved in a very short period of time;*
- *Impacting a significant number of businesses and or consumers;*
- *Impacting large geographic areas or regions;*
- *Impacting key government facilities, infrastructure and essential services;*
- *Impacting national security, economic security or public health and safety; and/or*
- *Likely to generate media coverage and or political sensitivities.*

Partner Bridge

means an operational virtual bridge to ensure nominated stakeholder representatives (refer to Table 1) are notified of a MSD and its impact, and provided with regular, timely updates on the impact and restoration progress. The Partner Bridge will also advise and facilitate the alignment of proposed media messaging.

2.3 Interpretations

In the Guideline, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of those;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act; and

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

3 FACTORS INFLUENCING THE SEVERITY OF MAJOR SERVICE DISRUPTIONS

The impact of an event on (or failure of) a system will vary depending on:

(i) The extent of the failure: How many people are affected? How large is the affected area?

(ii) The duration of the failure: How long are people affected for?

(iii) The location of the failure: Geographic locations are unique, for example isolated communities.

(iv) The time of the failure: Did the failure occur during a busy period or off-peak?

(v) Availability of alternative communications options: If only one network type is affected, are there alternative communications options still available?

(vi) Operating conditions at the time of failure: Is the network in normal operational mode or under high levels of load?

(vii) The level of organisational preparedness for the failure: Are appropriate procedures and resources available?

(viii) The level of individual and community preparedness?

(ix) To the extent a C/CSP has visibility of this, the level of industry preparedness, response, resourcing and equipment capabilities (including temporary facilities).

(x) The ability or inability of a C/CSP to gain access to a site or infrastructure due to State/Territory safety restrictions or classifications (floods, fires etc).

(xi) The availability of energy supply and/or access to fuel for onsite generators.

(xii) The ability or inability of a C/CSP to gain access to spare parts.

4 SEVERITY MATRIX

The following Severity Matrix has been established and may be used as guidance in addition to a C/CSPs own assessment framework for determining the severity of an MSD based on the impact to the community and the estimated time to remedy the effects of the disruptions. The impact to the community may be determined by a combination of factors including the number of technologies disrupted, other C/CSPs' network/infrastructure availability, population density, community isolation, number of services in operation, geography (island vs mainland etc.) and the infrastructure impacted.

Some examples have been included in the Severity Matrix to provide context as to the type of event that may be considered as having a severe impact to the community. In the table below, multiple networks could mean multiple technologies disrupted within one Carrier or could mean multiple instances of disruption to the same technology type (i.e. multiple Carriers) or both.

FIGURE 1
Severity Matrix

	Local (Based on postcode)	**Wide area effect**	**State / Territory**	**Communication method required**
Critical – long term event that may require >1 day to recover	No or very limited telecommunications capability in local area with more than one network affected.	No or very limited telecommunications capability over a wide area with more than one network affected.	All telecommunications inoperative in a significant portion of one or more States or Territories for one or more networks.	• Partner Bridge • Broadcast email • Online communication medium
Significant – medium term event that may take >4 hours to recover	No or limited telecommunications capability in local area with one or more networks affected.	No or limited telecommunications capability over wide area with one or more networks affected.	No or limited telecommunications capability in one or more States or Territories with one or more networks affected.	• Broadcast email • Online communication medium
Limited – short duration event (≤ 4 hours recovery)	No or limited telecommunications capability in a limited area with one or more networks affected.	No or limited telecommunications capability in a wide area with one or more networks affected.	No or limited telecommunications capability in one or more States or Territories with one or more networks affected.	• Broadcast email

The C/CSP impacted by the MSD is responsible for assessing the severity of the MSD based upon the Severity Matrix in Figure 1. Where an MSD affects more than one C/CSP, each C/CSP will make their own assessment of the severity of the MSD. The C/CSPs shall then discuss and agree the severity of the MSD and in the case that there is no agreement, the MSD will be classified as the highest level of severity identified.

5 COMMUNICATIONS PLAN

5.1 Key Stakeholders

There are a number of key stakeholder streams in the telecommunications eco-system. Communications within the Emergency Call Person (ECP) organisation are recognised as a separate stream. This Guideline sets out the information to be provided to each stream during a MSD.

In some cases, a C/CSP may identify a potential disruption to its networks impacting normal operations (e.g. cyber event). In other cases, Australian Government agencies will drive the response framework in a pre-planned and pre-agreed manner. This communications plan is intended to be the blueprint for the latter course of action.

TABLE 1
Communications Streams

Consumers	Users of telecommunications services, broadcasters
Emergency Call Person	Telstra (000, 112) Concentrix (106)
Emergency Service Organisations	Operational and senior management
Government	Includes but is not limited to: • Australian Cyber Security Centre • Department of Infrastructure, Transport, Regional Development and Communications • Department of Home Affairs • Emergency Management Australia • Crisis Coordination Centre • Critical Infrastructure Centre • Australian Government and their emergency management agencies. - NSW Telco Authority - Territory and Municipal Services Directorate - Northern Territory Emergency Service - QLD Disaster Management Committee - DPC Security and Emergency Management Committee SA - Dept of Police and Emergency management TAS - Emergency Management Victoria - State Emergency management Committee WA
Regulatory	Australian Communications and Media Authority Australian Competition and Consumer Commission
Telecommunications dependencies	Utilities (energy, financial, health services), Data Centre providers
Telecommunications suppliers and industry bodies	Carriers/CSPs Communications Alliance Australian Mobile Telecommunications Association (AMTA) Telecommunications Industry Ombudsman (TIO)

Note: A full list of stakeholders is detailed in Appendix A: Contacts Lists.

5.2 Major Service Disruption – Information Provision

Where a Carrier or CSP becomes aware of an MSD rated as critical in the Severity Matrix (see Figure 1) occurring or having occurred, an initial email containing the below information should be circulated to other C/CSPs. (A contact list for relevant parties is included in Appendix A).

(a) The cause and nature of the disruption;

(b) When the disruption commenced;

(c) The area(s) affected;

(d) The type of infrastructure and services disrupted;

(e) The estimated number of customers affected;

(f) Any essential services identified as being affected;

(g) The expected timeframe for the network/service being brought back to operation, and any temporary service arrangements if applicable;

(h) Other communication stream stakeholders to be engaged; and

(i) Any other information relevant to the MSD that other communication stream stakeholders need to be aware of.

Some types of MSDs, for example bushfires, are very dynamic situations. As such, reports (especially early report) of the likely scale and duration of an outage are often best estimates and, therefore, subject to change. It is recommended that C/CSPs caveat reports accordingly.

5.3 Communication Principles

Where an MSD occurs to telecommunications, the relevant key stakeholders within each respective communication stream will work closely together to minimise the impact on the disruption of telecommunications to the community. The communication method required will be based on the severity, as per the Severity Matrix in Figure 1.

The C/CSP impacted by an MSD should determine the most suitable mechanism for relaying information about the MSD and discussing impacts with key stakeholders, considering business-as-usual arrangements and arrangements put in place by Australian Government agencies to manage a disaster.

For MSDs rated as significant, or higher, the C/CSP should consider the MSD, its impacts, whether other C/CSPs would be experiencing a similar MSD and how best to discuss the MSD and its resolution with other key stakeholders.

This may be via a State/Territory emergency event Partner Bridge that may already be in operation, or to arrange a meeting using a unique bridge between C/CSPs and their partners/suppliers (where relevant).

In the case that multiple parties are affected by an MSD, the first C/CSP that initiates the conversation will be responsible for further activity to maintain lines of communication with key stakeholders throughout the event (unless otherwise agreed).

NOTE: Information provided by participants for guidance on partner bridges or other forums is shared for the purpose of implementing this guideline and should not be used by any recipient for any other purpose without the express consent of the disclosing participant.

Participants provide information under this guideline in good faith and consistent with the Objectives in section 1.3, however, no participant warrants the accuracy or completeness of this information as it is provided to the best of their knowledge at the time and under the circumstances outlined in this guideline and as such is released from any liability whatsoever in connection with the information provided.

For MSDs rated as limited, there may only be the need to advise stakeholders via a broadcast email. This may occur between C/CSPs, technical support groups etc.

Where appropriate, the public will be informed as to how to obtain further information on the impacts of an MSD. This may be via a variety of radio networks, emergency warnings from broadcasters or other network operators if roaming agreements are in place, and via public media announcements, stakeholder websites and social media channels.

The parties will work together to ensure information communicated to the public is clear and promotes community confidence in the telecommunications sector.

NOTE: The Department of Infrastructure, Transport, Regional Development and Communications will, as appropriate, advise the Minister for Communications, Cyber Safety and the Arts, the Minister for Regional Health, Regional Communications and Local Government and the Crisis Coordination Centre (Department of Home Affairs).

5.4 Contact List

All stakeholders and parties associated with the Guideline shall complete a contact list (see Appendix A) and provide contact details to Communications Alliance as soon as practicable and maintain and keep their contacts current. Communications Alliance will maintain the contact list on its website – www.commsalliance.com.au, with updates made within one Business Day of notification of the change. The contact list is password protected.

6 MANAGING A MAJOR SERVICE DISRUPTION

Generally, the Guideline contains processes for an all hazards approach. See section 7 and 8 for events with slightly different approaches such as cyber events or health-related events.

The Guideline recognises the importance of planning and the four distinct phases of a disruption to telecommunications services:

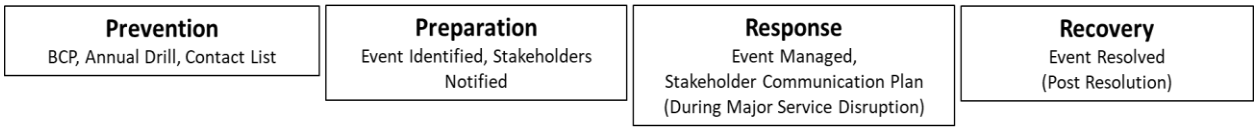
Prevention – to eliminate or reduce the impact an MSD causes to a service provider's ability to communicate details about the MSD with stakeholders;

Preparation – to enhance capacity of stakeholders and communities to cope with the consequences of emergencies;

Response – to ensure the immediate consequences of emergencies to critical infrastructure and communities are minimised; and

Recovery – measures which support C/CSPs' customers and communities affected by emergencies in the reconstruction of physical infrastructure.

FIGURE 2
Disruption Event Phases



6.1 Prevention

Prevention is the elimination or reduction of the risk to or severity of exposure to the consequences of an emergency or MSD.

For example, prevention of an MSD causing a disruption to the ability to communicate with external stakeholders would be having a satellite phone or some other form of communication in place.

6.2 Preparation

This phase addresses the preparation, planning and skills training for staff in order to mobilise structures and resources to support a response to and recovery from an emergency or MSD. C/CSPs should:

- Arrange emergency/disaster management training for relevant staff;
- Develop and regularly review business continuity plans (BCPs). This may include understanding interdependencies between stakeholders and consideration of integrated planning or exercises between organisations;
- Plan, conduct and participate in regular testing of disaster management arrangements, emergency management exercises and review of BCPs;
- Update and share material components of individual BCPs with Australian Government agencies;

- Co-ordinate, in advance of the likely disruption to services, based on proactive communications received from key stakeholders – e.g. extreme weather conditions affecting power supply etc;
- Ensure the necessary representatives or teams within the organisation are familiar with their respective State emergency management plans;
- Ensure the necessary representatives or teams within the organisation are familiar with the contents of this Guideline; and
- Complete and maintain the contact list under Appendix A with the necessary contact details of staff as soon as practicable.

6.3 Response

This phase outlines the ability to communicate with key external stakeholders in the event of an MSD, in order to keep individuals, the community and key stakeholders aware of the status of network restoration.

The key actions for all stakeholders during this phase include:

- Providing the MSD information as per section 5.2 to the relevant communications streams;
- Participation in the Partner Bridge (or other forum) (see section 6.3.1) which will be facilitated and co-ordinated by the relevant Australian Government agency or C/CSP; and
- Providing administrative and logistical support to staff and equipment during the MSD.

6.3.1 Partner Bridge (or other forum)

During an MSD, a Partner Bridge (or other forum) may be set up, subject to the type of MSD and its distribution. The Partner Bridge may be established by a C/CSP, an Australian Government agency or in some instances, the energy sector. Notifications of the Partner Bridge details will be provided to contacts (Appendix A) via an SMS/email alert.

Apart from the overall stakeholder Partner Bridge/forum which includes all stakeholder streams, there may also be the need for additional Partner Bridges/forums to be set up and hosted regularly, or for C/CSPs to join other forums (such as State control centres) where they exist.

Where there are other pre-existing forums, these are to be used in preference to establishing separate, concurrent Partner Bridges, to ensure centralisation and coordination of activities and communication, and to avoid duplication, gaps or conflicting communication.

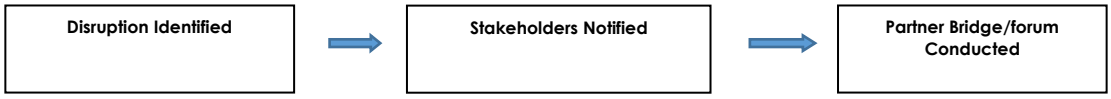
Regardless of whether Partner Bridges are established by C/CSPs, or whether the C/CSPs attend pre-existing forums, they should attempt to address the key elements listed further below.

A summary of the Partner Bridge/forum outcomes, action points and details of any approved media messages will be sent out

to nominated participants as required, following each Partner Bridge/forum. This will be done by the incident manager facilitating the Partner Bridge/forum.

Stakeholders are to ensure that a nominated representative from their organisation is in attendance at each Partner Bridge/forum.

FIGURE 3
Partner Bridge



Disruption Identified: Confirm that the Partner Bridge/forum should be convened as per the Severity Matrix (see Figure 1).

Stakeholders Notified: An alert will be sent advising that there is a disruption, confirming that the disruption is under investigation, and notifying the stakeholders to call into the Partner Bridge/forum number at a nominated time.

Partner Bridges/Forum Conducted: During an event there may be one or more Partner Bridges/forums convened. Each Partner Bridge/forum will be opened with a roll call. Details of the incident, the start time, the impact (geographical, call type, complete or partial/intermittent failure), and investigation details to date will be provided by the Bridge/forum facilitator.

Expectations of duration and restoration will also be communicated as available. Appropriate media messaging may be discussed. The expected start time for any subsequent Partner Bridge/forum (if applicable) will be notified on each call and confirmed at a later time.

A typical agenda would likely include:

- Roll call;
- Technical update on cause and expected duration (as understood);
- Discussion on impact;
- Proposed media messaging;
- Summary of agreed action items and responsibilities
- Close and details of subsequent Partner Bridge/forum (if applicable).

Note: Some stakeholders may audio-record these Bridge conversations, as part of their normal process.

6.4 Recovery of Service

The recovery of service phase is marked by the restoration of communications capabilities to customers.

When the MSD has ended, a post-disruption checklist should be completed by C/CSPs and advised (if required) via a final Partner Bridge/forum, that the network has returned to a service operation environment. If restoration is to continue over a period of time, this is noted and planned.

In summary, a C/CSP should;

- complete an end-to-end test and checklist (refer table 2 below).
- Check downstream systems.
- If required, participate in a final Partner Bridge/forum to confirm that the disruption is resolved and that services are restored.
- Communicate to the media (as necessary) that disruption is resolved, and services are restored.
- Complete a Post Incident Review and convene a review meeting if required. Learnings to be documented and incorporated into the stakeholder BCPs and this Guideline as appropriate.

At the close of the final Partner Bridge/forum, participants will be advised of the resolution and that no further bridges will be convened for the specific event. Bridge invitees will also receive an advice confirming this.

TABLE 2

Network Disruption Recovery checklist

Recovery Checklist	
☐	Confirm impacted Technology Alarms/Events Cleared.
☐	Confirm telecommunications services have been restored, or that no further action required.
☐	Confirm network performance has returned to BAU or is in progress and no further action required by partner members.

6.5 Reporting - Carrier and CSPs with wholesale channels

Information on the number of end-users affected by the MSD should be ascertained as part of the reporting on the MSD event.

The number of end-users affected may be identified by the CSP.

Or, where the CSP is in a relationship with a wholesale provider the CSP may have prior arrangements in place for the management of reporting the number of affected end-users to be via the wholesale partner, or by each wholesale partner where that CSP may have arrangements with more than one wholesale partner for different network products.

To avoid over-reporting, Carriers with wholesale channels should not report numbers of affected end-users, unless by prior agreement between the wholesale supplier and the CSP.

NOTE: Some Carriers are also prevented from reporting specific end-user details in forums (including emails and reports) where staff in the Carrier's retail channel would have visibility of these details. This includes, for example, Telstra's Structural Separation Undertaking.

7 CYBER EVENT

A cyber event, such as a mass spam event, Denial of Service (DoS) or Distributed Denial of Service (DDoS) event (including machine generated PSTN traffic, ransomware, malware) or other cyber event (intended or unintended) is recognised as a particular style of interruption. Suspected cyber events will be actioned by the affected network provider(s).

NOTE: G644:2020 Emergency Call Service Protections Requirements Guideline, details processes and communication messages associated with a DoS or DDoS event on the Emergency Call Person (ECP) and in the case of a misalignment between this Guideline (G663:2020) and G644:2020, the latter takes precedence.

The primary purpose of G644:2020 is to mitigate the effects of an event affecting call traffic to Triple Zero or the ECP.

If a cyber event is confirmed, the C/CSP will inform the ACMA and the Australian Cyber Security Centre (ACSC) of the event.

Cyber events should be notified to the ACSC via:
https://www.cyber.gov.au/acsc/report

In the event of a cyber event C/CSPs will;

- work with other C/CSPs to maintain the integrity of the telecommunications network throughout a cyber event;
- identify the caller impacts that arise due to a cyber event; and
- follow an effective communications strategy to inform stakeholders and the community and provide suggested media messaging.

Technical and stakeholder Partner Bridges may be convened as per usual Disaster Management processes.

For further information on various cyber events, the ACSC has developed a *Strategies to Mitigate Cyber Security Incidents – Mitigation Details* document along with other useful publications. It is recommended that stakeholders access the ACSC website and familiarise their organisations with the information on the implementation of the mitigation strategies.

While some of these strategies may not be targeted at MSDs, some cyber events, such as business email compromise and threats to industrial control systems, could have the potential to become an MSD if left unmitigated.

8 HEALTH-RELATED EVENTS

A health-related event, such as the outbreak of a severe flu, pandemic or other significant threat to human health (intended or unintended) is recognised as a particular style of MSD. For example, during a pandemic, telecommunications services may remain unaffected, but the resources required to operate and maintain telecommunications services may well be impacted. Response to suspected health-related events will be actioned by the network provider and will follow the general processes of this Guideline, although communications messages will differ slightly.

9 REFERENCES

Publication	Title
Industry Codes	
C536:2011 Incorporating Amendment No.1/2015	*Emergency Call Service Requirements Industry Code*
Industry Guidelines	
G644:2020	*Emergency Call Service Protections Requirements*
Legislation	
Privacy Act 1988	
Telecommunications Act 1997	
Telecommunications (Consumer Protection and Service Standards) Act 1999	
Telecommunications (Emergency Call Service) Determination 2019	
Emergencies Act 2004 (ACT)	
Emergency Management Act 2013 (NT)	
Disaster Management Act 2003 (QLD)	
Emergency Management Act 2004 (SA)	
Emergency Management Act 2006 (TAS)	
Emergency Management Act 2013 (VIC)	
Emergency Management Act 2005 (WA)	
State Emergency and Rescue Management Act 1989 (NSW)	
Essential Services Act 1988 (NSW)	

APPENDIX

A CONTACT LISTS

Critical Communications Contacts List

All stakeholders and parties associated with the Guideline shall complete the contact list below and provide those details to Communications Alliance as soon as practicable and maintain and keep their contacts current.

Communications Alliance will host a consolidated list on its website – www.commsalliance.com.au, with updates made within one business day of receiving notification of the change at info@commsalliance.com.au. The contact list is password protected.

Authority / Organisation / Utility	Representative	Position	Email	Contact (Fixed/Mobile)	State Location

Energy Supplier Contact List

A separate telecommunications / energy supplier contact list will be established and completed by relevant stakeholders.

Both Communications Alliance (CA) and Energy Networks Australia (ENA), as the respective industry bodies, will host the up to date contact list within their member portals. The lists should be completed and kept up to date with any necessary changes being notified to both CA and ENA as soon as practicable.

B Protocol for Notification of Major Service Disruptions

The *Protocol for Notification of major service disruptions* (Protocol) sets out how the Department will liaise between industry and the Minister for Communications, Cyber Safety and the Arts and the Minister for Regional Health, Regional Communications and Local Government (Ministers), in the event of a Major Service Disruption.

The Protocol requires telecommunications industry members to report Major Service Disruptions to the Department as soon as practicable by email to: cialerts@communications.gov.au and ccc@homeaffairs.gov.au.

The Protocol takes an 'all hazards' approach – that is, it applies where there is a major service outage, regardless of the cause. The cause of an outage may not be known until sometime after the event.

The Protocol can be accessed via the Trusted Information Sharing Network (TISN) Communications Sector Group (CSG) or the Department.

NOTE: C/CSPs should continue to liaise directly with State and Territory-based agencies in an emergency.

See Appendix D for a Major Service Disruption notification template.

C Crisis Coordination Centre

Emergency Management Australia is a division of the Department of Home Affairs.

Emergency Management Australia is home to the Australian Government Crisis Coordination Centre (CCC). The all-hazards, 24/7 centre provides whole-of-government situational awareness to inform national decision-making during a crisis.

The CCC also coordinates physical Australian Government emergency assistance and manages the National Security Hotline, vital to Australia's national counter-terrorism efforts.

State and Territory Governments manage emergency responses in their jurisdictions. The CCC coordinates the Australian Government physical and financial support for disasters and emergencies.

Emergency Management Australia is guided by the National Strategy for Disaster Resilience.

Telecommunications industry members should report MSDs to the CCC as soon as practicable by email to: ccc@homeaffairs.gov.au.

D Notification of Major Service Disruption

Below is a sample template for a Major Service Disruption notification developed by the Department and as used in the Protocol.

Notification of Major Service Disruption

Name of Organisation

As at [00:00hrs, Day Month Year]

All new information is shown in italics

Status of event:	e.g. Initial / Update / Resolved	
Date first notified:	Time and Date of first notification	
Nature of event:	e.g. Natural hazard / failure of asset or system / CT	
Location of event/incident:	State: Region/s: Suburb/s:	
Details of event, if known:	If known, cause and chain of events.	
Services impacted:	Describe the types of services and approximate number of users impacted	
Estimated time to resolve:	If known	
Next update expected:	Approximate time update to be sent to the Department	
Actions undertaken:	Include details about: contact with media outlets and other agencies, requests for assistance received from government agencies and other organisations Activation of recovery or response arrangements	
Authorisation		
Prepared by:	Name Position	0000hrs Day Month 2016
Contact Officer:	Name Position	P M E
For general enquiries please contact: [email]		

PARTICIPANTS

The Working Committee that developed the Guideline consisted of the following organisations and their representatives:

Organisation	Representative
AMTA	Lisa Brown
CISCO	Kim Yan
Enex Testlabs	Matt Tett
NBN Co	Fiona McGrath
NBN Co	Cameron Scott
NEXTDC	George Dionisopolous
NSW Telco Authority	Simon Fruend
NSW Telco Authority	Peter Williams
Optus	Quinton Meiring
Telstra	Paul Harrison
Telstra	Michael Ryan
TPG Telecom	Alexander R. Osborne
Vocus	Jonathan Gleeson

This Working Committee was chaired by Alexander R Osborne. Craig Purdon of Communications Alliance provided project management support.

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507