



Te Tari Taiwhenua

Date 16 September 2005

PO Box 805  
Wellington  
New Zealand

Website [www.dia.govt.nz](http://www.dia.govt.nz)

**REQUEST FOR INFORMATION**

**DIA 2005/28**

**Title:** **UNIFIED MESSAGING SYSTEM for NATIONAL CDEM WARNING SYSTEM - Ministry of Civil Defence & Emergency Management**

**Closing Date and Time:** **Thursday 6 October 2005 at 12 noon.**

**Tender Delivery Instructions:** Responses are to be enclosed in a sealed envelope clearly marked **“RFI No. DIA 2005/28 - UNIFIED MESSAGING SYSTEM – Ministry of Civil Defence & Emergency Management”** and must reach the Contracts & Services Manager at the address below by the closing time specified.

**Submission of Proposals:** Proposals in response to this RFI must be delivered as follows:

Attention: Contracts & Services Manager  
Department of Internal Affairs  
Level 1  
46 Waring Taylor Street  
PO Box 805  
WELLINGTON

**On Behalf of:** Ministry Of Civil Defence & Emergency Management (MCDEM)

**Contact for Inquiries:** Bruce Tichbon  
Consultant for MCDEM  
Phone Direct 021 388 324  
btichbon@paradise.net.nz  
C/O Consultel Associates Ltd  
PO Box 2097  
Wellington

**Deleted:** (the Consultant)

**RFI DIA 2005/28**

# Contents

<b>1. Glossary of Terminology .....</b>	<b>3</b>
<b>2. General Background Information.....</b>	<b>4</b>
2.1 Purpose.....	4
2.2 Background.....	4
<b>3. Administration .....</b>	<b>6</b>
3.1 Submission Instructions.....	6
3.2 Communications.....	6
3.3 Terms and Conditions.....	6
3.3.1 Confidentiality.....	7
3.3.2 Reliance on Information.....	7
3.3.3 Potential Partnering Notification.....	7
3.3.4 Conflict of Interest.....	7
3.3.5 Undisclosed Benefits.....	7
3.3.6 Further Information.....	8
3.3.7 Evaluation and Notice of Outcome.....	8
3.3.8 Response Costs.....	8
3.3.9 Non Conforming Response.....	8
3.3.10 Rights Reserved.....	8
3.3.11 Presentation.....	9
<b>4. Business Requirements.....</b>	<b>10</b>
4.1 Integration.....	10
4.2 Outputs.....	10
4.3 Inputs and Control.....	10
4.4 Template management.....	10
4.5 Address List maintenance.....	10
4.6 Confirmation of receipt.....	11
4.7 Compliance.....	11
4.8 Security.....	11
4.9 System Availability & Support.....	11
4.10 Architecture.....	11
4.11 Implementation & Maintenance.....	11
4.12 Reference sites.....	11
4.13 Other potential.....	11
<b>5. Respondent Information.....</b>	<b>13</b>
5.1 Company Details.....	13
5.2 Company Contact.....	13
5.3 References.....	13
<b>6. Technical Information.....</b>	<b>14</b>
6.1 NCMC IT Architecture.....	14
<b>7. Relevant Government IT and Security Initiatives.....</b>	<b>15</b>
7.1 SSC Development Goals.....	15
7.2 e-government Initiative.....	15
7.2.1 e-GIF.....	15
7.2.2 GSN.....	15
7.2.3 Online Authentication.....	15
7.2.4 Directory.....	15
7.3 GCSB Requirements.....	15
7.4 Security in Government Sector (DPMC).....	15
<b>Appendix 1 .....</b>	<b>16</b>

## 1. Glossary of Terminology

CAP	Common Alerting Protocol - the OASIS standard for homeland security and civil emergency management. CAP is a data interchange format for collecting and distributing "all-hazard" safety notifications and emergency warnings over information networks and public alerting systems. The current version is CAP v1.1
CCIP	Centre for Critical Infrastructure Protection
CDEM	Civil Defence and Emergency Management
DIA	Department of Internal Affairs
DMS	DMS DIA Document Management System
e-GIF	E-government Interoperability Framework - a collection of policies and standards endorsed for NZ government IT systems.
EMA; EMA's	<b>MCDEM</b> Emergency Management Advisors (located in Auckland, Wellington and Christchurch).
ESA data standard	<b>E</b> mergency <b>S</b> ervices and government <b>A</b> dministration – geospatial data standard for NZ e-GIF purposes. Defines common geographical locators.
GCSB	Government Communications Security Bureau
GML	Geography Markup Language (GML) is an application of XML built on XML schema. It models, transports and stores geographic data. ISO has adopted GML as the ISO 19136 standard. GML is part of the e-GIF.
GSN	Government Shared Network
LINZ	Land Information New Zealand
MCDEM	Ministry of Civil Defence and Emergency Management
NCMC	National Crisis Management Centre
NDO	National Duty Officer (MCDEM)
NWS	National Warning System
NZSIT	New Zealand Security Information Technology standards (publications) issued by GCSB. (Such as NZSIT 400).
OASIS	Organization for the Advancement of Structured Information Standards- a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards.
PSTN	Public Switched Telephone Network
PTWC	Pacific Tsunami Warning Centre
SEEMail	Secure Electronic Environment - government environment designed to facilitate the exchange of email and attachments using the Internet. This system is capable of protecting public domain information and information classified IN-CONFIDENCE, SENSITIVE and RESTRICTED.
SIGS	Security in Government Sector <u>(per DPMC – Department of the Prime Minister and Cabinet)</u>

## 2. General Background Information

### 2.1 Purpose

The Ministry of Civil Defence & Emergency Management (MCDEM) require a system to improve the National CDEM Warning System (NWS) through more effective dissemination of information, receipt of confirmation (acknowledgement) and address list maintenance.

The purpose of this RFI is to conduct a market scan of service providers capable of providing unified messaging (fax/email/txt/voice) options for the purpose of the dissemination of alerts/warnings by MCDEM.

The focus is on finding fast, simple, multiple, cost effective yet robust ways to communicate urgent, relatively short messages of information for the purpose of warnings by MCDEM. It will also look at better ways for recipients to confirm receipt of warnings to MCDEM as well as more effective recipient address list maintenance.

Implementation of any upgrade- if decided- is expected in 2006.

Formatted: Highlight

### 2.2 Background

MCDEM administer and maintain the NWS under the CDEM Act 2002, the National Civil Defence Plan and the proposed National CDEM Plan.

The NWS is designed for the dissemination of warnings from the national level on any type of threat. National warnings are most likely to emanate from alert notifications received by MCDEM from a range of information agents via the MCDEM Alert Notification System. Local authorities maintain local warning systems to disseminate warnings as received from the NWS (MCDEM) further into the communities, as well as for the purpose of localised (non-national) warnings.

Deleted: (not only those related to typical civil defence/natural disaster events).

National Warning messages are currently sent to:

- MCDEM EMA's
- Local level CDEM (Territorial Authorities & regional councils/CDEM Groups)
- The 3 Police Communications Centres
- NZ Fire Service
- Ministry of Health
- Airways Corporation
- Rescue Coordination Centre NZ (MSA)
- If required - Radio & TV - selected stations through individual MOU's.

Deleted: MCDEM is responsible for the dissemination of among other, national tsunami warnings. The requirements for the effective communication of tsunami warnings are used as the benchmark to base planning and design of the NWS upon, as warning effectively on tsunami will cover effective warning on any other type of threat also.

Deleted: The NWS is tested 4 times per year through national warning test messages - two tests within and two outside normal office hours.

Deleted: district

National warning messages can potentially be sent to other government agencies and national lifeline utilities, depending on their capability to receive and acknowledge them as per the NWS procedures.

#### Current processes

Alerts that may trigger a national warning message are received by the MCDEM 24/7 National Duty Officer (NDO) in different ways and formats, depending on the source of the information. Typical sources are the Pacific Tsunami Warning Centre in Hawaii (phone, fax, email & txt), MetService (fax & phone), Institute of Geological & Nuclear Sciences – GNS (phone, fax, email & txt) and the public/local authorities (phone).

Formatted: Bullets and Numbering

Deleted: and problems

Deleted: An average of about 500 such individual alerts are received and noted/considered annually by MCDEM. Other departments may also be sources (e.g. Ministry of Health for a virus outbreak).

National warning messages are sent by the MCDEM National Duty Officer via fax, email and txt (txt is only an alert that a warning has been passed, and refers the recipient to their fax or email).

MCDEM needs to be able to activate the NWS (send warnings) from anywhere at any time. Warning message templates are kept on MS Word files currently stored on DIA's Document Management System, duty officers' personal USB drives, laptops etc.

Recipients of national warning messages are required to acknowledge receipt within 30 minutes (by a person authorised to deal with the message). Currently this acknowledgement is done via phone calls to the MCDEM duty officer (who may use a call centre arrangement to take & note the confirmations) or the MCDEM EMA's in the respective regions. The call centre & EMA's then compile a report to the MCDEM duty officer, noting all the acknowledgements and times. Police assist with tracing those at local levels that did not acknowledge and could not be reached.

A central address list containing all recipient addresses (phone, cell/pager, fax, and email) is maintained by MCDEM and is sent to all participants, after quarterly tests of the NWS, for updating.

**Deleted:** Currently different systems are used for each mode of communication. In practice this implies multiple separate processes to send a warning. The original logic behind this approach was based on redundancy considerations, which proved useful when for instance the fax service was down at the time of a warning test. However, it is the contention that better ways of disseminating messages are possible without compromising redundancy.¶

**Deleted:** Access to DIA's central IT systems is however required for using both the electronic fax and email systems. Currently DIA IT security measures (via Telecom NZ Safecom) for remote access to its systems slow the process up significantly and does not make for guaranteed remote access at all times. Subsequently MCDEM tries to send all messages from the National Crisis Management Centre's infrastructure, but in reality that will not always be possible or practical.¶

**Deleted:** DMS (

**Deleted:** )

**Deleted:** This implies the requirement of meticulous management every time changes to templates are made to ensure that the versions on all these files are updated.¶

**Deleted:** the

**Deleted:** quarterly (

**Deleted:** each test)

**Deleted:** This central list is filed on DMS. Each individual communication system used to send warnings (voice, fax, email & txt) however requires additional and separate maintenance of its own address lists. The data for these lists are manually entered as taken from the central list. The current system proved effective but inefficient and may be prone to failure in that five separate lists require maintenance. The effective maintenance of these lists is subsequently dependent on meticulous management and control by a single designated person, posing a further risk from a continuance point of view.

## 3. Administration

### 3.1 Submission Instructions

Responses are due by **06 October 2005 at 12 noon**. Three printed copies (two bound and one unbound) and one electronic copy in MS Word version 2000 format on CD should be provided in a sealed envelope.

It is recommended that responses are restricted to a few pages only (no more than 10 A4 double sided pages). Responses should be clear, and sufficiently detailed to allow an objective evaluation.

Formatted: Bullets and Numbering

Responses should be delivered to:

**Contracts & Services Manager  
Department of Internal Affairs  
Level 1  
46 Waring Taylor Street  
P.O. Box 805  
WELLINGTON**

Responses must be marked '**Commercial - In Confidence. RFI No. DIA 2005/28 UNIFIED MESSAGING SYSTEM for NATIONAL CDEM WARNING SYSTEM – Ministry of Civil Defence & Emergency Management**'

DIA accepts no responsibility for lost or misdirected responses.

DIA reserves the right to accept or decline late responses at its sole discretion.

Responses received by DIA will become the property of DIA.

### 3.2 Communications

All communication regarding this RFI, including requests for clarification or additional information, must be directed in writing (via email) to:

Bruce Tichbon  
Consultant for MCDEM  
Phone Direct 021 388 324  
btichbon@paradise.net.nz  
C/O Consultel Associates Ltd  
PO Box 2097  
Wellington

Deleted: (the Consultant)

Respondents should not contact any other DIA/MCDEM employee or agent regarding this RFI without first gaining specific written permission from Bruce Tichbon.

The dialogue with suppliers will continue during the period up to and beyond the RFI closing date.

Formatted: Bullets and Numbering

### 3.3 Terms and Conditions

In responding to this RFI, vendors must acknowledge their agreement to the terms and conditions outlined in this document.

### 3.3.1 Confidentiality

Any documents submitted by DIA to Respondents are to be treated as strictly confidential and are to be used by the Respondent only in relation to the preparation of the RFI. All responses submitted by Respondents shall be treated as confidential and will not be returned.

The entire RFI process, including communications, is confidential to DIA and the particular respondent. No advertising, press release or other information relating to this RFI or the subsequent invitation for RFP shall be published or otherwise made public without the prior written consent of DIA. Copies of this document, or parts thereof, are to be restricted to the respondent's staff or the staff of organisations associated with the respondent's proposal. This information is not to be used for any other purpose, or disclosed to any party not directly involved in the preparation of the proposal.

Respondents shall ensure that the same conditions strictly apply to any person or organisation the respondent communicates with in the course of preparation and submission of the RFI.

The above requirements are in addition to the requirements under any separate confidentiality agreement or non-disclosure agreement that may arise between DIA and respondents.

All communications, including responses, from vendors regarding this RFI will be treated as confidential, subject to DIA obligations under the Official Information Act 1992 or any other enactment or rule of law.

### 3.3.2 Reliance on Information

DIA will rely on information provided by, or on behalf of, respondents for the purpose of this RFI. In providing information, respondents represent to DIA that the information is complete and accurate in all material respects, which it is not misleading and that in preparing the information all reasonable skill and care has been exercised.

Respondents will be deemed to have informed themselves fully on the requirements of the RFI and the work required and no costs will be accepted arising from a failure to observe this condition.

### 3.3.3 Potential Partnering Notification

Well prior to the submission of your proposal you are encouraged to discuss with DIA any potential partnering arrangements with other organisations.

### 3.3.4 Conflict of Interest

Any potential conflicts of interest should be declared in writing to DIA immediately. Failure to do so is likely to lead to disqualification of the proposal.

Formatted: Bullets and Numbering

### 3.3.5 Undisclosed Benefits

Respondents must not directly or indirectly provide any form of inducement or reward to any representative of DIA involved in this project.

### **3.3.6 Further Information**

DIA may at any time during the evaluation process, contact any respondent/s for clarification or further information about their response. Under these circumstances, questions, answers and other information is not required to be circulated to every respondent.

### **3.3.7 Evaluation and Notice of Outcome**

Responses will be considered on the basis of:

- The fit of the proposed service to the requirements
- The ability of the provider to deliver the required service
- Confidence in the ability of the service provider to establish and maintain a mutually satisfactory business relationship
- The completeness and quality of the response
- Compliance with the RFI instructions
- Reference checks results
- Cost implications

DIA/MCDEM has absolute discretion in:

- Determining any evaluation processes
- Whether it invites any of the respondents for tender/RFP

DIA/MCDEM will inform all respondents of the outcome of this RFI process by November 2005.

### **3.3.8 Response Costs**

DIA will not be liable for any costs incurred in the preparation or submission of responses.

Respondents will be responsible for any costs incurred in relation to the preparation, execution and completion of their responses.

### **3.3.9 Non Conforming Response**

Where a response is incomplete or in the wrong format DIA will advise the respondent that the response is incomplete and DIA reserves the right to consider or reject any non conforming response at its sole discretion.

### **3.3.10 Rights Reserved**

DIA reserves the right to:

- issue written amendments to this RFI, including varying the specified requirements
- suspend or cancel this RFI process, in whole or in part, at any stage prior to completion, without incurring any liability or cost
- accept or decline any or all responses or enter into negotiations with one or more respondents
- alter any date or time in the RFI process with reasonable notice
- apply whatever weight it wishes to any criteria relating to evaluating responses
- issue the RFI to any organisation it chooses

### **3.3.11 Presentation**

DIA may invite short listed vendors submitting responses to individually present their company and services.

## 4. Business Requirements

Respondents are requested to make point-by-point responses to the requirements below. Respondents are requested to give detailed costs of their solution, and detail the trade-off of functionality versus cost.

A clear architectural description is to be given, particularly detailing the physical locations of the various components so that the impact of failure of different components and networks (or channels) can be assessed (ie PSTN, mobile networks, Internet, etc).

Formatted: Bullets and Numbering

This document describes the current method of operation and MCDEM's future intentions. Any alternative ideas or visions are welcome.

Formatted: Bullets and Numbering

Deleted: vision

### 4.1 Integration

A simple and integrated solution that meets the NWS specification of a unified multi media solution for dissemination of warning messages.

Formatted: Bullets and Numbering

### 4.2 Outputs

Current output message formats are:

- Voice
- e-mail
- fax
- text
- the systems must be able to accommodate other formats that may be added in future (instant messaging, CAP, RSS, GML etc are being discussed in the industry)

Formatted: Indent: Left: 72 pt, Bulleted + Level: 1 + Aligned at: 108 pt + Tab after: 126 pt + Indent at: 126 pt

### 4.3 Inputs and Control

Effective and reliable access (for creating and sending messages, system management etc) is required, especially remote access. The current range of access media include:

Formatted: Bullets and Numbering

Deleted: More e

- phone (fixed PSTN and mobile)
- fixed PC (located at MCDEM/NCMC or anywhere else)
- mobile laptop PC
- access using PDA like devices is a new requirement (laptops are proving bulky and inconvenient)
- generally access by web browser with suitable authentication seems the most flexible option, but other options would be considered.
- the systems must be able to accommodate other formats that may be added in future (such as instant messaging, CAP, RSS, GML etc are being discussed in the industry)

Formatted: Indent: Left: 72 pt, Bulleted + Level: 1 + Aligned at: 108 pt + Tab after: 126 pt + Indent at: 126 pt

Formatted: Indent: Left: 72 pt, Bulleted + Level: 1 + Aligned at: 108 pt + Tab after: 126 pt + Indent at: 126 pt

### 4.4 Template management

Effective message template access & maintenance. (Note that text and voice message content will always be a different to fax and email content, so these may have to be grouped together).

Formatted: Bullets and Numbering

Deleted: More effective

### 4.5 Address List maintenance

Effective address list maintenance and management (integration). A single database or address list is required. The ability for NWS alert recipients to update their own contact details on the integrated database/address list is desirable.

Formatted: Bullets and Numbering

Deleted: More effective

#### 4.6 Confirmation of receipt

Easy confirmation (acknowledgement) of receipt of messages, noting that confirmation must be by a person and not only system generated. Acknowledgements are required and acknowledgement lists are kept and audited after real warning messages and tests.

Deleted: Potentially easier

Formatted: Bullets and Numbering

#### 4.7 Compliance

Suppliers are to ensure any systems provided comply with relevant government IT, communications and security initiatives (many of which are detailed in Section 7).

Formatted: Bullets and Numbering

#### 4.8 Security

Suitable system security and access authentication is required in the NWS system, especially where remote access is used. Because of the danger of the NWS system security being compromised, two-factor authentication (one time password generator) may be required. It is envisioned that this can be provided using the 'All-of-government Authentication programme' due to be available 2006. In the meantime single factor authentication will probably be used as an interim measure.

#### 4.9 System Availability & Support

Acceptable levels of system availability (99.9%) are required. It is envisioned that 24x7x365 support may be necessary.

Deleted: It is not clear whether a simple piece of shrink-wrapped software will meet most/enough of the requirements, or if a more 'enterprise grade' solution will be required.

Formal Service Level Agreements (SLA's) may be required.

Formatted: Bullets and Numbering

#### 4.10 Architecture

A range of architectural options is potentially available to meet service level requirements. A suitable solution could be a service or an in-house solution. The architecture could potentially consist of one, two or all three of the following hosting options (suitably designated primary site, disaster recovery site etc).

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

- Hosting by a service provider
- Hosting of server by a third party in a suitably robust site
- Hosting of server at the NCMC site in the Beehive (this has obvious advantages of robustness if external networks fail).
- Integration with government and DIA/National Crisis Management Centre (NCMC) IT architectures (current and future) is possibly required.

Formatted: Indent: Left: 92.15 pt, First line: 0 pt, Bulleted + Level: 1 + Aligned at: 108 pt + Tab after: 126 pt + Indent at: 126 pt, Tabs: Not at 126 pt

Deleted: Currently, a Crisis Management System (CMS) for NZ is being scoped.

#### 4.11 Implementation & Maintenance

The following issues are to be detailed:

- Implementation/deployment plans
- Testing plans
- Training
- Operational issues
- Support plans
- System development, and integration issues
- Helpdesk

Formatted: Bullets and Numbering

Formatted: Indent: Left: 90 pt, Bulleted + Level: 1 + Aligned at: 126 pt + Tab after: 144 pt + Indent at: 144 pt

#### 4.12 Reference sites

Reference sites are required - NZ customers or, if the solution is not used in NZ, Australian customers are to be described. Note – there are sovereignty and control issues with NZ government data being kept offshore.

Formatted: Bullets and Numbering

#### 4.13 Other potential

The system is to potentially provide a standard for MCDEM to lead the CDEM industry to limit the proliferation of different warning systems and to attempt to collapse the multi-

Formatted: Bullets and Numbering

level warning hierarchy depicted in Appendix 1. This is not viewed as a critical requirement, yet the potential of a future solution to accommodate such integration is regarded as worthy of consideration.

**Deleted:** important

## 5. Respondent Information

### 5.1 Company Details

Provide a brief overview of your organisation, including:

- Years in existence/ experience
- Size, staffing and location(s)
- Types of services offered

### 5.2 Company Contact

Provide contact details, including:

- company name and title
- company address
- contact name
- telephone numbers
- fax number
- e-mail address

### 5.3 References

Reference information will be treated with the utmost confidentiality. Proven performance is a significant evaluation criteria.

Any contact with the reference sites will be arranged by the Respondent and be made by DIA during the RFP evaluation

## 6. Technical Information

### 6.1 NCMC IT Architecture

The NCMC, which is located in the basement of the Beehive in Wellington, is manned during civil defence emergencies. There is a case (but it does not exclude other possibilities) for locating an NWS server in the NCMC environment where external network failures will not isolate the NDO from the server.

**Formatted:** Bullets and Numbering

**Deleted:** and is the primary location for MCDEM staff at such times.

The NCMC has been configured as a Windows 2000 Domain named NCMC.GOV.TZ. There are two domain controllers located in the NCMC. There is also an additional server located in Auckland which is available for DR purposes. Lotus Notes cluster configuration is supported.

**Deleted:** basement

**Deleted:** MCMC

**Deleted:** basement

**Deleted:** server room named NCMC01 and NCMC02.

**Deleted:** called NCMC03

**Deleted:** basement

There is a secure SEEMail server in the NCMC.

Access to the site (external security) is via Telecom NZ's Safecom service. Cisco PIX firewalls provide internal security. An external Web server sits behind a DMZ. There is a backup Web server in Auckland. The NCMC primary servers have no Web presence.

There is no public access to the core environment. Only lead government departments have access to the core via physical links.

DIA provides support for DIA/NCMC operations only.

**Deleted:** Currently the

**Deleted:** during normal business hours (8-5pm Mon-Fri)

**Deleted:** Outside of these hours there is currently no support provided.

## **7. Relevant Government IT and Security Initiatives**

Formatted: Bullets and Numbering

Suppliers are to ensure any systems provided comply with relevant government IT, communications and security initiatives. A selection of the initiatives is shown below.

### **7.1 SSC Development Goals**

Formatted: Bullets and Numbering

The government development goals can be viewed at:  
[www.ssc.govt.nz/display/document.asp?NavID=242&DocID=4730](http://www.ssc.govt.nz/display/document.asp?NavID=242&DocID=4730)

Relevant goals are:

#### **Goal 3: Networked State Services**

Use technology to transform the provision of services for New Zealanders:  
By June 2007: Networks and Internet technologies are integral to the delivery of government information, services and processes.

By June 2010: The operation of government has been transformed through the use of the Internet.

#### **Goal 4: Coordinated State Agencies**

Ensure the total contribution of government agencies is greater than the sum of its parts:  
By 2007: Government agencies demonstrating improvement through Managing for Outcomes, including joint outcomes and other shared accountabilities across clusters of agencies.

By 2010: Measurable results are evident from the joint pursuit of joint outcomes.

### **7.2 e-government Initiative**

Formatted: Bullets and Numbering

#### **7.2.1 e-GIF**

e-GIF v2.1 is the current standard. e-GIF v3.0 will be published soon.  
[www.e.govt.nz/interoperability/index.asp](http://www.e.govt.nz/interoperability/index.asp)

#### **7.2.2 GSN**

[www.e.govt.nz/gsn/index.asp](http://www.e.govt.nz/gsn/index.asp)

Formatted: Bullets and Numbering

#### **7.2.3 Online Authentication**

[www.e.govt.nz/authentication/index.asp](http://www.e.govt.nz/authentication/index.asp)

Formatted: Bullets and Numbering

#### **7.2.4 Directory**

Thinking is just starting on this. Up-to-date agency contact details are already available via the government intranet.

Formatted: Bullets and Numbering

### **7.3 GCSB Requirements**

[www.gcsb.govt.nz](http://www.gcsb.govt.nz)

The latest New Zealand Security Information Technology publications just issued by GCSB is NZSIT 400

The GCSB has recently released a new policy and security note on the use of BlackBerry by the New Zealand Government.

Formatted: Bullets and Numbering

### **7.4 Security in Government Sector (DPMC)**

Manual available at [www.security.govt.nz](http://www.security.govt.nz)

Formatted: Bullets and Numbering

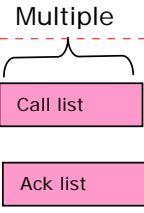
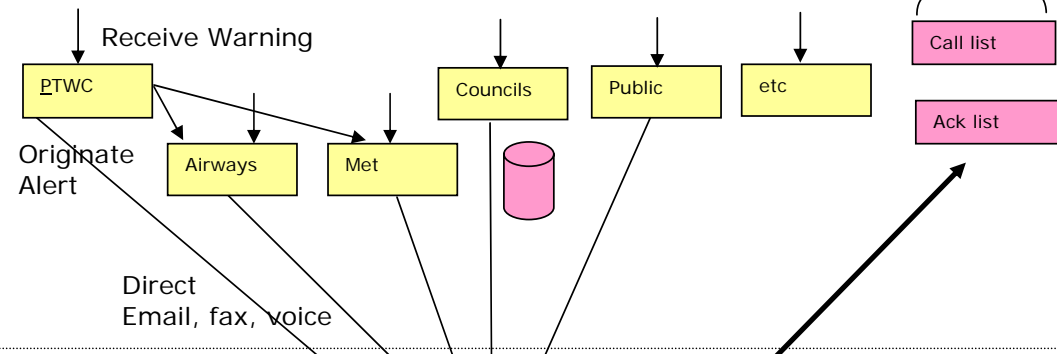
# Appendix 1

## Notes to Appendix 1

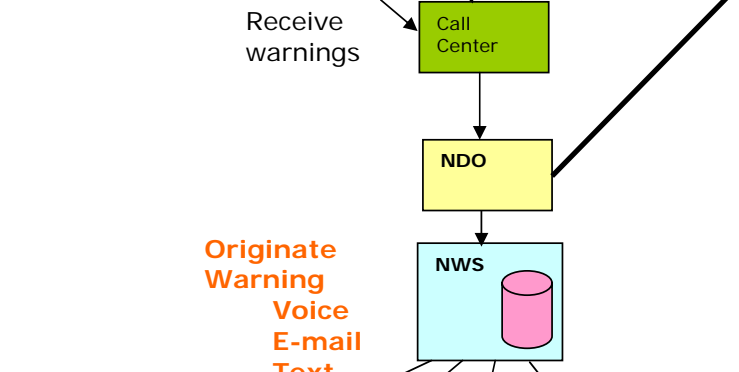
1. The general hierarchy is shown, but many message paths are left off for simplicity.
2. Messages generally follow the hierarchy but exceptions occur, eg shown as an exception is PTWC communicating directly with the NDO and also using Airways and Meteorological Service (Met) as additional relays.
3. There is repetition of messages to help ensure reliability. A recipient may receive the same important alert several times through several different media.

# Appendix 1 Alert Notification Flows

Deleted: Message

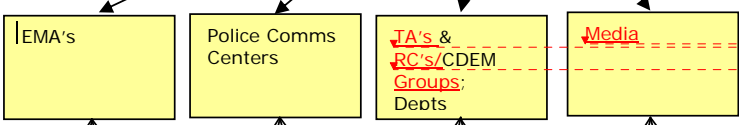


Originate Warning  
Voice  
E-mail  
Text



Formatted: Bullets and Numbering

Formatted: Indent: Left: 18 pt, Hanging: 9 pt, Bulleted + Level: 1 + Aligned at: 45 pt + Tab after: 63 pt + Indent at: 63 pt



Deleted: etc

Deleted: District

Deleted: Regional Councils

