FUJITSU

Disaster Resilience
The ICT Option

Submission for the Queensland Floods Commission of Inquiry

4th April 2011

Table of Contents

Document Control and Contact

Document Name	Disaster Resilience - The ICT Option
Confidentiality	External
Document Status	Final
Version Number	1.0
Summary	Submission for the Queensland Floods Commission of Inquiry
Authors	James Nockels, Paul Case and Ben Huntsman
Contact	[redacted]
Version Date	4th April 2011

Disaster Resilience – The ICT Options

As employees of Fujitsu Australia we are making this submission to the Commission of Inquiry into the Queensland Floods as a background paper to assist it in understanding the broad range of Information and Communications Technologies currently available to support crisis management. It is hoped that the Commission will find this a useful reference document when considering how the broad challenges of Crisis Preparedness, Response and Recovery can be supported by current technologies.

1 The Problem

Government agencies, non-governmental organisations, and community leaders globally face the challenging task of designing and implementing policies, programs, and systems that help local communities cope with a wide range of contemporary crisis situations. In societies like ours this task is often compounded by associated problems such as aged, overburdened, and complex critical infrastructure systems, urban spread and a growing magnitude of potential catastrophes not previously seen.

The idea of building a resilient response to natural and man-made disasters is now a dominant strategic theme in Australian crisis management. COAG's 2009decision to adopt a whole-of-nation resilience-based approach to disaster management recognised that the growing complexity of disasters extends beyond the emergency management community alone. Thus, a national, coordinated and cooperative effort is now being developed to enhance Australia's capacity to withstand and recover from disasters.

Even with unlimited resources, it is highly unlikely that a community can totally prevent or protect itself from all the possible dangers it may face. The sheer complexity of Australia's government, communications, power, water and distribution systems raise coordination and management challenges across jurisdictional boundaries. Individuals and organisations build their everyday activities around complex systems over which they have little control, such as electricity, computerised systems, and communication networks. Each of these modern systems allows communities to function more efficiently, yet few people maintain a stockpile of food and water or possess alternative modes of transportation, power generation, or communication in the event of an emergency.

Meanwhile, governments, communities, and individuals are equally ill prepared for disturbances to infrastructure, vital resources, or public goods and services. Part of the problem is that the efficiencies inherent within these complex systems of modern life reduce resilience through a loss in redundancy and diversity. Another aspect is that few systems are designed with resilience as a specification positively aligned to public expectations. The ability of these systems to be prepared for and recover from a disaster has a direct impact on the ability of a community to respond and recover. It is thus important to consider all the resources that a community can count on when assessing resilience.

That said the Internet and Social Networking and Media have become prolific, generic, and resilient communication networks that in many ways remain untapped by Government in times of crisis.

2 The Prevention, Preparedness, Response and Recovery Model

To respond to these challenges the Australian emergency management PPRR (Prevention, Preparedness, Response and Recovery) model recognises the need for:

- Prevention: to hinder, deter and mitigate disasters, while maintaining readiness to deal with disaster events.
- Preparedness: to protect people, assets, infrastructure and institutions from disaster events; and to establish, training and exercise arrangements to respond to, and recover from a disaster event.
- Response: to respond rapidly and decisively to a disaster event and manage its immediate consequences.
- Recovery: to return national and community life to normal as quickly as possible after a disaster event, through the restoration of social, economic, physical and environmental wellbeing.

In 2004 the *COAG National Inquiry on Bushfire Mitigation* further developed and adapted the PPRR framework to a 5Rs framework—Research, information and analysis; Risk modification; Readiness; Response; and Recovery—which it saw as a better basis for understanding the integrated elements of bushfire mitigation and management.

It added that application of the 5Rs framework should be informed by a thorough understanding of the full range of assets that are threatened by bushfire—life, property, infrastructure and production systems, environmental values and management.

This modification is equally applicable to any emergency management model as it places enhanced emphasis on the “up front” requirement for information and its analysis.

The PPRR model and its variants recognises that disaster resilience is a collective responsibility of all sectors of society, who by working together will be more effective than any individual effort. COAG has recognised that a disaster resilient community is one that works together to understand and manage the risks that it confronts, but is also aware of the responsibility of all levels of government. Thus, an associated challenge in achieving this goal is the need to ensure a coordinated whole-of-government and whole-of-community approach across Federal, State/Territory and Local governments.

2.1 Prevention

In anticipating and preparing for crises policy makers need a succinct, well balanced, analysis of what could happen, where and when it might happen and what they might need to do to circumvent the possible events. They need assessments that describe not only the nature and probability of future paths of events but also possible diversions from those paths and the identification of signposts that will tell them they are entering this new territory. The information they need must summarise what is known, structure the remaining uncertainties and provide useful guidelines for how they might be handled.

In addition there is a need to clarify the likely consequences of policies and actions as well as answer questions and provide information on issues not well understood. In doing this we need to remember that the specialist analyst often has access to more facts than those facing the challenge of developing relevant policy. In this situation the sum total of expert knowledge needs to be brought to bear in a structured, creative and predictive fashion.

Government's needs to know the likelihood of a critical event, and its possible nature and scope, so that it can begin to shape a continuous process of coordinated planning to deter such an event or effectively respond if one did occur. They also need to know about the predictable outcomes of various possible events so as to sharpen the detail of their security planning.

Currently government at all levels is not well served in this area with few sources of centralised accesses to all information relevant to this important risk management function. Each sector of national endeavour needs to be analysed to ascertain its vulnerability and potential for remediation action. This will include the known types of threat to each sector, the nature of past crises, the location of likely threat occurrences in Australian and their possible vulnerability.

The sectors which need to be covered and addressed include:

- **Government infrastructure**
  - Federal, State and Local
- **Communications**
- **Banking and Financial Institutions**
- **Water Services**
- **Transportation Networks and Systems**
  - Aviation
  - Surface Transport
  - Maritime
- **Energy Sector**
  - Electricity
  - Gas and oil producers and distributors
- **Health**
  - Hospitals
  - Pharmaceuticals manufacturers and distributors
  - Ambulance Systems
  - Local doctors
- **Emergency Services Organisations**
  - State/Territory/Federal
  - Non-government providers
- **Food Chain**
  - Growing regions
  - Food importation and Distribution Systems
  - State/Territory/Federal Agriculture Departments
  - Major food distributors and retailers

- **Hazardous Materials and chemicals producers and shippers**

Elements of these essential categories are currently covered under the Australian Government Critical Infrastructure Resilience Strategy where participants undertake implementation of the strategy in their own business area. But there is no central data repository or data linking system that will provide a single overview of point for all threats assessed, risks enumerated and remediation taken.

This situation is paralleled in the government sector where, again, there are no readily available central overview point (dash board) on the range of threats and remediation action taken in response across the range of government interests.

Unlike Australia's preparations for countering terrorism, the emergency management system has no agreed need for a single, unified, information collection and processing capability and data base standards. There is no endorsed system that is structured to deliver assessed information – *Intelligence* - for the prevention planning, preparedness coordination and response and recovery management in emergency management. Although this is now being addressed in a number of forums, by example the Ministerial Council for Police and Emergency Management and the Royal Commission into the Victorian Bushfires.

Over a number of years the Police and Military have used "intelligence led" operations to some effect. There is a view that suggests Information (read intelligence) Led Emergency Management is gaining momentum. This is driven in part and assisted by increased sharing of information and greater interoperability.

Information and data, and their analysis and synthesis, are the basis for knowledge and learning from which emergency managers can continuously improve the effectiveness and efficiency of the risk management process and in particular mitigation and response management. Consistent data gathering and collation about likely emergency situations across Australia have been limited, handicapping informed decision making.

As an example, spatial data and its use in mapping products have become increasingly important for emergency mitigation and management. Advances in technology, analytical tools and communication (such as the increasing availability and quality of satellite remotely sensed data and its interpretation and communication to diverse audiences) are very important to event mitigation and management. While some action is in hand progress towards consistent, widely available data and information anomalies and gaps remains an issue. Issues include a national program of fire and flood regime mapping and the establishment and maintenance of emergency related data bases at local, State and Federal levels which are consistent and linked.

Commissioners may therefore wish to consider whether emergency managers need to have access to an "intelligence" system similar to that used in the national counterterrorism arrangements which refines information and creates intelligence to prepare for and manage counter terrorist situations. Such a system would have the ability to gather disparate information on a range of likely threat situations and allow the risk generated to be assessed and logged, remediation proposed and progress in implementation documented.

The creation of local operationally based "intelligence cells" would collect, collate and evaluate locally gathered information to produce evaluated data for local planning and operational requirements. These cells would support broader State wide risk assessments and input verified data into regional and State emergency management centres. In the first case they would provide enhanced risk coordination capacities by centralising the collection, collation and processing of large scale and diverse relevant data.

2.1.1 Risk Assessment

Determining the nature of the threat scenarios the State is likely to encounter, both natural and human, requires a Risk Assessment process at various levels of Government and key private industry. The underlying requirement of such a process is to assess the risk of an emergency affecting a geographical area or areas that threatens serious damage to human welfare.

The fundamental process consists of seven sub-elements:

- The threat component enables identification of the types of crises that need to be protected against; their likelihood, how they might be manifested and where they are likely to occur.
- The criticality element permits a general rating as to their relative importance and the creation of hierarchy of criticality those points to areas and assets requiring protective measures.
- The vulnerability component evaluates the amount of protection or resilience an area or asset has as compared to the possibility of a critical event.
- The response and recovery element measures the capability to respond to and recover from each crisis event.
- The impact (or consequence) part of the assessment measures the critical significance of loss that would occur due to a crisis event.
- The risk component demonstrates a hierarchical rating of the result of the threat, vulnerability, and impact analysis
- The needs component permits a review various protection and recovery solutions that would serve to reduce the level of risk of a crisis event.

This process ensures that emergency managers have an accurate and shared understanding of the risks that they face so that remediation planning has a sound foundation and is proportionate to the risks by providing:

- a rational basis for the prioritisation of objectives and work programmes and allocation of resources both Government and non-Government;
- a means of assessing the adequacy of plans and capabilities,
- highlighting where existing measures are appropriate,
- gap identification;
- facilitating joined-up local planning based on consistent planning assumptions;
- provide an accessible overview of the emergency planning and business continuity planning, and
- Assessments that support emergency planning and capability development.

Complex emergency management equations are amenable to ICT solutions supported by tools which can draw together the large amounts of data necessary to build a threat picture while overlaying it on critical community elements and their vulnerabilities. Such data pictures can be developed at local, first responder, level and aggregated at high coordination levels to an ultimate State level data holding. Such data holdings can provide a State wide picture of risk management action and also monitor the state of remediation action across the State.

Such a data base would form the nucleus of a State crisis management data repository with the capacity to add preparedness, response and recovery information necessary for the management of an emergency. The data repository would hold the core information necessary for the management of a crisis and has the capacity to become the key element in a total State emergency management system. In addition it can be made available to cooperating adjacent State and Federal agencies that may need to become involved if the emergency is of major proportions.

Such data bases now operate within and across, for example, police jurisdictions providing "data truth". An example can be seen in the Crimtrac National Police Reference System – Persons. This is in essence a national repository of information derived from disparate Police data sources and available to assist in a variety of police investigations.

2.2 Prepare

Having gathered the data necessary for an assessment of emergency risks and undertaken the remediation action deemed necessary and feasible emergency planning then requires a commitment to preparing for an emergency. By developing a sound understanding of, and managing, the assessed risks emergency managers then need tools to undertake a range of preparedness tasks that can be powerfully supported by ICT.

2.2.1 Information and Communications

Information is critical to emergency preparations, response and recovery. Yet gathering it and maintaining its flow within agencies, with partners and to the wider public, is extremely challenging in the preparation phase as well as under emergency conditions. However the importance of information to emergency responders and those affected by events cannot be underestimated. It is, in fact, the first crucial platform of the emergency management process.

Information is critical to emergency response and recovery and its collation, assessment, verification and dissemination must be underpinned by appropriate information management systems. These systems need to support single and multi-agency decision making and the external provision of information that will allow members of the public to make informed decisions to ensure their safety.

Information systems also need to be coordinated to be effective, both within organisations and between organisations and at all levels (i.e. local, regional and national) in order to produce a coherent, integrated effort.

An effective information management system is dependent upon appropriate preparatory measures being in place to build situational awareness and the development of a common operating picture. It provides such information to meet local, regional and state levels (if appropriate). Such measures need to support:

- the transmission and collation of potentially high volumes of information from multiple sources;
- the assessment of collated information to ensure its relevance, accuracy, timeliness, accessibility, interpretability and transparency; and
- The translation of available information into appropriate information products, for example, briefing strategic coordinators at the regional or state level, or release to the media for public information.

Its end product is an assurance that emergency response coordinators have correct, corroborated, information on which to base their decisions and actions.

To discharge their responsibilities emergency managers have a requirement to gather and store information relevant to the management of any crisis. Broad categories of data include:

- Volunteer management – who are they, where are they, what is there level of training, how can they be contacted etc.?
- Pre Positioned Supplies – what has been stockpiled, what commercial sources are available, who owns them, how can they be contacted etc?
- Evacuation Planning – what areas might areas need to be evacuated, how will this occur, where might evacuees go etc?
- Safe Haven Management – where are they, who owns them, who manages them, what communications do they have etc?
- Casualty Prediction – which events might produce causalities, what might be the symptoms, where might they be treated etc?
- Community Outreach – what communities exist in the likely emergency areas, how are they managed, what are their contacts, what communications exists etc?
- Mobilisation/exercising- scenarios, training programs, exercise schedules, learning outcomes etc.

This is not to say that all disparate systems across the agencies need or should be the same as differences in operational and administrative requirements may preclude it. The important issue is the sharing of relevant information in a timely and collaborative fashion. The previously mentioned Crimtrac system achieves this for a particular business requirement but as the information becomes more complex and time critical the sophistication of the data exchange and use increases. This situation is epitomised in the counter terrorist situation where disparate and widely sourced information needs to be quickly collated, analysed and assessed for truthfulness and utility. The well developed and exercised system of Joint Intelligence Groups and the National Intelligence Group provides an excellent model for this as does its supporting ICT infrastructure and analytical tools.

There is a view that ICT systems are now becoming “Enterprise”, meaning the information held in various intra agency systems needs to perform in concert and also interact with other agencies. The traditional approach is that operational systems, for example geospatial mapping tools would not necessarily interact with say the agency’s payroll and rostering systems. This is now being challenged as richness of information is required for decision makers; “Are the people available at the town rostered on and trained to perform the task?”

Preparing for training and exercising for this has generally been a manual practice with incident team and managers working traditional paper based models to test the effectiveness of systems and practices. As the complexity of information sharing and interoperability increases so will the need to test the systems and practice the individuals within the new paradigm. There are a range of existent commercial products now available that facilitate more effective training and exercising. These are used in a number of jurisdictions to support regular cost effective exercising using the internet to link staff in their existing work environment in a virtual exercising environment.

2.3 Response

Having been constructed to anticipate and prepare as best as possible for an emergency a well-constructed emergency management data base would have the data and interconnectivity to support effective response management.

When an emergency occurs, those responsible for managing the response and recovery effort will face an array of competing demands and pressures. These will vary according to the event or situation that caused the emergency, the speed of its onset, the geographical area affected, any concurrent or interdependent events and many other factors.

Information on the emergency will often be incomplete, inaccurate or ambiguous, and perceptions of the situation may differ within and between emergency responders.

The response and recovery effort may involve many organisations, potentially from across the public, private and voluntary sectors, and each will have its own responsibilities, capabilities and priorities that require co-ordination.

The objectives of emergency managers focus on delivering outcomes relating to:

- saving and protecting human life;
- relieving suffering;
- containing the emergency – limiting its escalation or spread and mitigating its impacts;
- providing the public and businesses with warnings, actionable advice and information;
- protecting the health and safety of responding personnel;
- safeguarding the environment;
- protecting property as far as reasonably practicable,;
- maintaining or restoring critical activities;
- maintaining normal services at an appropriate level;
- promoting and facilitating self-help in affected communities;
- facilitating investigations and inquiries (e.g. by preserving the scene and effective records management);
- facilitating the recovery of the community (including the humanitarian assistance, economic, infrastructure and environmental impacts);
- evaluating the response and recovery effort; and
- Identifying and taking action to implement lessons learned.

Meeting these responsibilities in an informed, flexible and effective way depends on positive engagement and information sharing between all agencies and at all levels. It also needs to be undertaken at a very fast tempo and interesting circumstances.

In such circumstances integrated ICT systems offer high speed data processing capabilities that can facilitate the performance of emergency management tasks using a range of tested applications. These include features that:

- Integrate and overlay information from different domains, facilitating the fusing of information, in both tabular, graphical, and geospatial presentation views.
- The ability to filter and provide different information and mixes of information for different operational roles. To prevent information overload and clutter.
- Provide information that enhances and empowers the decision making process.
- Provides actionable intelligence and understanding.

- Facilitates the enhancement of information by specialists and analysts and the seamless presentation and integration of this value enhanced information into a fused view.
- The integration of check lists, standard operational procedures, plans, and the actions taken into a common workspace for each operational role.
- Detailed information of all asset classes, the related acquisition and logistics information.
- Enhanced logging and the linking of logging to enable a clear understanding of what has just occurred, and the history of what occurred and what action was taken, for de-brief, analysis, learning, and legal requirements.
- Enable subject matter experts, and different agencies to work collaboratively and in de-centralised locations to manage the emergency.
- Provide a seamless ability to communicate to and from frontline responders, other control centres and partner agencies, using multiple media, data and sensor information types.
- The ability to communicate via multiple channels to the community on a mass or individual basis, and to track the messages and their relationship to the response plan.
- Tools within the system to provide quality measures, to be used as part of a quality management and outcome measurement.

As well as this wide array of commercially available ICT tools we also draw attention to the potential to make greater use of the Internet, Social Networking and Media. These are powerful tools that the Commission might consider could be leveraged to enhance emergency management, response and cope with excessive peak demands. During the recent earthquake crisis in Japan large scale outages of more traditional communications networks saw the news media and individuals using Twitter, Facebook and Skype to not only report the crisis but advise Government and families of their safety and or predicaments.

The Internet is a key communication back bone being both resilient and open. To understand its communicating power we need only turn to the current situations in Egypt and Libya where governments turned it off to stop the rapid exchange of information. While we recognise that embracing the Internet and Social Media does introduce some security challenges for agencies managing emergencies we are also aware that adequate operational and security systems are available to provide appropriate protection and assurance.

2.4 Recovery

Recovery is understood as the process of rebuilding, restoring and rehabilitating the community following an emergency, but it is more than simply the replacement of what has been destroyed and the rehabilitation of those affected. It is a complex social and developmental process rather than just a remedial process. The manner in which recovery processes are undertaken, managed and communicated is critical to their success. An additional complexity is that local communities may also look upon an emergency as an opportunity to regenerate an area. This regeneration phase may overlap with the recovery phase.

Experience in many countries has shown that the recovery phase and the structures, processes and relationships that underpin it are less well known and usually complex and long running.

Recovery involves many more agencies and participants than the response phase and is often a complex intertwining of Local, State and Federal government and non-government infrastructure providers responsibilities.

It will also be more costly in terms of resources, and will be the subject of close attention by the community, the media and government. It is therefore essential for the process to be based on well thought out and tested structures and procedures for it to work in an efficient and orderly manner. It is also necessary for decisions and actions to be based on adequate information and analysis of the cost and implications of decisions.

Because of its social and economic significance to the community and its strong psychological impact recovery phase needs to begin at the earliest opportunity following the onset of an emergency, running in tandem with the response to the emergency. It will then continue until the disruption has been rectified, demands on services have returned to normal levels, and the needs of those affected (directly and indirectly) have been met. In this process information, specialist services and resources are key players.

Crucial elements in the recovery process are:

- Planning and management arrangements, which are accepted and understood by recovery agencies, the community and armed forces (if deployed) and their data inputs and reporting are aligned.
- Recovery management arrangements and their information management support need to comprehend the complex, dynamic and protracted nature of the processes and the changing needs of affected individuals, families and groups within the community over time.
- The management of recovery is best approached from a community development perspective with the active participation of the affected community and effective communication tools are needed to support this.
- Recovery management is most effective when agencies involved in human welfare have a major role in all levels of decision-making which may influence the wellbeing and recovery of the affected community – again requiring effective data exchanges and linkages.
- Recovery is best achieved when the recovery coordination managers are engaged the moment the emergency begins.
- Recovery planning and management arrangements are most effective where they are supported by training programmes and exercises which ensure that the agencies and groups involved in the recovery process are properly prepared for their role.
- Recovery is most effective where its management arrangements provide a comprehensive and integrated framework for managing all potential scenarios.

In this situation systems used to manage emergencies need to dove tail and become an integral part of recovery. Existing ICT systems which can deliver this capability have the following generic features:

- Provide a warehouse of recovery program information from government, non-government and sub-contracted organisations.
- Provide a linked inventory of recovery programs and projects, providing the ability to roll up and drill down in to the detail of individual recovery projects.
- The ability to track actual progress of the planned projects,
- Provide traffic lights and dashboards to in power decision makers with information to adjust, refine and re-prioritise the response programs.
- Tools and databases to systematically manage victim, casualty information and processes. Maintaining the links to the incidents, communities and locations.

- Provide methods to communicate and engage with the community via multiple channels, gauge opinion and arrange and co-ordinate meetings, briefings and gain requirements.

Emergency management and recovery should be taken forward in tandem from the outset, although in some cases constraints on capacity may necessitate a degree of separation, with the recovery effort gathering momentum once the initial risk to life has been mitigated.

3 Conclusion

Emergencies create business continuity challenges. Demands on staff time, resources and management attention will be significant while maintaining the response and recovery effort alongside an organisation's day-to-day functions will pose a major challenge. The risk of senior management discontinuity during prolonged periods of pressure may not be immediately apparent, but can be significant. These issues can, however, be more easily managed through good organisation, planning and thorough training, at every level. These basic management processes are all capable of being enabled by ICT systems which allow easily accessible and verifiable data bases, linked communications and reporting systems, easy identification of available trained staff and physical resources and integrated command and control systems.

Integrated data bases supported by commercially available software applications can provide a continuous stream of verified and usable data to support the full emergency management PPRR spectrum. They can also link, using a wide variety of communications systems, local responders through the whole command chain to state level and even federal emergency agencies. Such systems can also draw in diverse data sources including emerging data sources, particularly geospatial information.

It is also clear that the internet and its emerging social networks have a key role in emerging emergency management systems. Governments will need to begin to take steps to embrace their use as citizens and working level emergency responders see systems such as Twitter, Facebook and Skype.

By investing in a more integrated approach to the use of ICT in emergency management the following benefits could be achieved:

- Greater Anticipation & Prevention of Emergency & Disaster Risks & Threats to meet Government and Community demands for better management of emergency & disaster related risks and hazards.
- Improved Agency & Community Preparedness by providing greater cross agency alignment around mission, planning, collaboration, capability, training, structure & assets.
- Situational Awareness & Complete Situation Picture Integrated into the Emergency Management Lifecycle by providing real time, accurate, consistent & shared data, information & intelligence
- Improved Resilience – Response, Recover & Rebuild by creating a more responsive and coordinated secondary emergency & disaster response, as well as greater focus on community recovery

Should the Commission wish to seek clarification or elaboration of any aspect of our submission we would be pleased to assist.