C2 Interoperability – An Australian National Whole of Government Approach

9th International Command and Control Research and Technology Symposium

Electronics and Aerospace, IS3

ADI

Agenda

- Setting the Scene
- Aim
- Interoperability including Technical and Operational
- Imperatives of Interoperability, including Cases Studies
- Security Issues
- Conclusion

- Not an Official Australian Government View
- Vision from Defence Industry Viewpoint
- Case Studies undertaken using public domain information

Australia?

- Large Country - 7,617,930 sq km
- Small Population – 19,913,144
- Interior Mostly Uninhabited
- Communications Infrastructure mostly in Populated Areas
- Large Coastline - 25,760 km

Setting the Scene

- Recent events both in Australia have shown that defence forces are increasingly being used to assist in of civil crises and national emergencies.
- The Australian government needs to be able to implement procedures that allow available civil and military resources to be marshalled and coordinated effectively.
- With a wide range of organisational cultures it is not practical to impose the same command and control procedures across all organisations, military or civil.
- More productive and sensitive approach is to determine how to promote interoperability across this community in a way that is affordable and reasonably non- intrusive.

Aim

- To examine the concept of interoperability as it applies to cooperation amongst a mixture of Australian national organisations and agencies
- Identify key issues that need to be understood and addressed.

Technical Interoperability

- Technical Interoperability can be defined as the ability of systems, to provide to and accept services from other systems and to use the services so exchanged to enable them to operate effectively together
- Technical interoperability can be addressed through agreeing appropriate technical standards that allow technical interfaces to be determined and, if resources allow, addressed

Operational Interoperability

- Concept introduced by the Australian Defence Science and Technology Organisation (DSTO) to cover the higher-level issues characterised by human-activity.
- Organisational interoperability stresses the organisational and cultural aspects rather than the technical, systems and operational aspects of interoperability.

Four enabling attributes of organisation interoperability formed the basis of the model:

- **Preparedness:** What doctrine, experience and training enable the organisations to work together?
- **Understanding:** What level of information and knowledge sharing exists and how is the information used?
- **Command Style:** How are roles and responsibilities delegated or shared? and
- **Ethos:** What level of trust, culture, values and goals are shared?

Australian Defence Strategic Review 1993:

In time of conflict, the Government should be able to implement a **unified national response** in which available civil and military resources could be marshalled and effectively coordinated. …… It also **calls for a civil military interface in the theatre of operations**, to coordinate implementation of our national response. **Arrangements for coordinating Federal, State and Territory policy making and advice need to be better defined and practised**.

- Several recent Australian Case Studies:
  - Canberra Bushfires of 2002
  - Regional Assistance to the Solomon Islands
  - Pong Su Incident
  - Counter Terrorism Exercises in Australia

Canberra Fires of 2002 - Background

- Bushfires in Australian are a seasonal hazard and great efforts are placed in the prevention, preparedness, response and recovery from bushfire incidents.
- On Saturday 18 January 2003 Bushfires, which had been burning in the hills to the west and southwest of Canberra for more than a week, reached the perimeter of the city.
- Widespread damage to rural properties, parks and forests, more than five hundred houses were destroyed along with significant urban infrastructure (Power, Telephones, Water Supplies and Gas)
- Four people died.
- Drought and weather were major factors in the spread of the fire.

Canberra Fires of 2002 – Organisations Involved

- Australian Capital Territory (ACT) Emergency Service Bureau, including the ACT Fire Service, ACT Ambulance Service and ACT Bushfire Service;
- Australian Federal Police, who provide policing for the ACT;
- New South Wales (NSW) Rural Fire Service;
- Victoria Country Fire Authority (CFA);
- Emergency Management Australia, in the coordination of assistance from interstate and federal agencies;
- Department of Defence (DOD), providing heavy equipment, manpower and Aircraft; and
- Many other Government Departments and Non Government Aid Agencies

Canberra Fires of 2002 – Communications

- Radio communications systems did not meet the substantial demands created by an event of this magnitude” .
  - Inadequate coverage;
  - Congestion on various networks;
  - Overwhelming of the communication centre;
  - Apparent shielding, possibly because of dense smoke;
  - Inadequate ground–air communication;
  - Difficulties with interoperability between the various firefighting elements; and
  - Insufficient quantities of equipment.
- Participants used communications equipment of different types that were incompatible.

Canberra Fires of 2002 – C2 Arrangements

- Operation was directed from the ACT ESB Operations Centre,
- Other operations centres involved (Defence, NSW RFS and Victorian CFA) did not have easy and simple procedures and technology for interaction.
- Problems within the command and control relationship between the ACT Fire Brigade and ESB existed as well as differences in the command and control philosophies of the ACT and New South Wales bushfire services.
- The Incident Control System (ICS) arrangements in New South Wales are more aligned to the national approach.
- By contrast, ACT bushfire brigade captains have greater operational independence and responsibility.

Canberra Fires of 2002 – Conclusion

From an examination of the responses mounted to the Canberra fires, it can be concluded that problems with interoperability existed at both the technical and operational level. On the technical level radios and information systems were for the most part incompatible. Organisational interoperability was actually non existent.

Assistance to the Solomon Islands - Background

- Over the period from 1998 to 2003, ethnic tension and violence caused the deterioration of the rule of law in the Solomon Islands until most aspects of government, including hospital, schools and policing ceased to exist.
- The Government of the Solomon Islands' loss of control was widely acknowledged across the community and a request for external intervention was subsequently sanctioned by a unanimous vote of the Solomon Islands Parliament.
- The Regional Assistance Mission to Solomon Islands, or RAMSI, was subsequently created to provide a solution. Under RAMSI the deployment of about 300 police officers, backed by 1700 military personnel, from nine regional countries (Australia, New Zealand, Fiji, PNG, Tonga, Samoa, Vanuatu, Kiribati, and Cook Islands) was undertaken to stabilise the situation.

Assistance to the Solomon Islands – C2 Arrangements

- Tactical communications presented a problem between civilian elements (AFP and APS) and Australia Army and Naval units.
- Tactical Communications between all participating military units also created a problem
- The initial use of the LPA HMAS Manoora, which has command ship capabilities, provided operational communications back to the Australian Headquarters and established a ready made operational and tactical command post.

Assistance to the Solomon Islands - Conclusions

- Technical interoperability from tactical to operational level did not exist or was very poor. There also appeared to be a lack of organisational interoperability.
- Interoperability at the operational level appears not to have been addressed.

Pong Su Incident - Background

- Victorian Police observed the Tuvala registered, North Korean owned, freighter Pong Su close to the Victorian Coast.The next morning, the two suspects were apprehended at their hotel with 50 kgs of pure heroin.
- In a subsequent search of the beach, Australian police discovered the body of a North Korean recently buried close to a dingy.
- The Pong Su led Australian police vessels on a four-day chase in 30-foot swells until commandos boarded the freighter by helicopter and boat. Australian authorities ordered the Pong Su into harbour, but the ship attempted to escape into international waters. After a helicopter boarding by the Australian Defence Forces SASR, the Pong Su was brought into port.

Pong Su Incident

Pong Su Incident - Organisations Involved

The agencies involved with this operation were:

- Victoria Police, using internal information systems;
- Australian Federal Police; using PROMIS ; and
- Department of Defence, especially Special Forces using a combination of the Joint Command Support System (JCSS) and the Special Operations Command Support System (SOCSS).

None of these organizations shares a common information system at the classified level nor has any systems interconnect to provide the transmission of classified information.

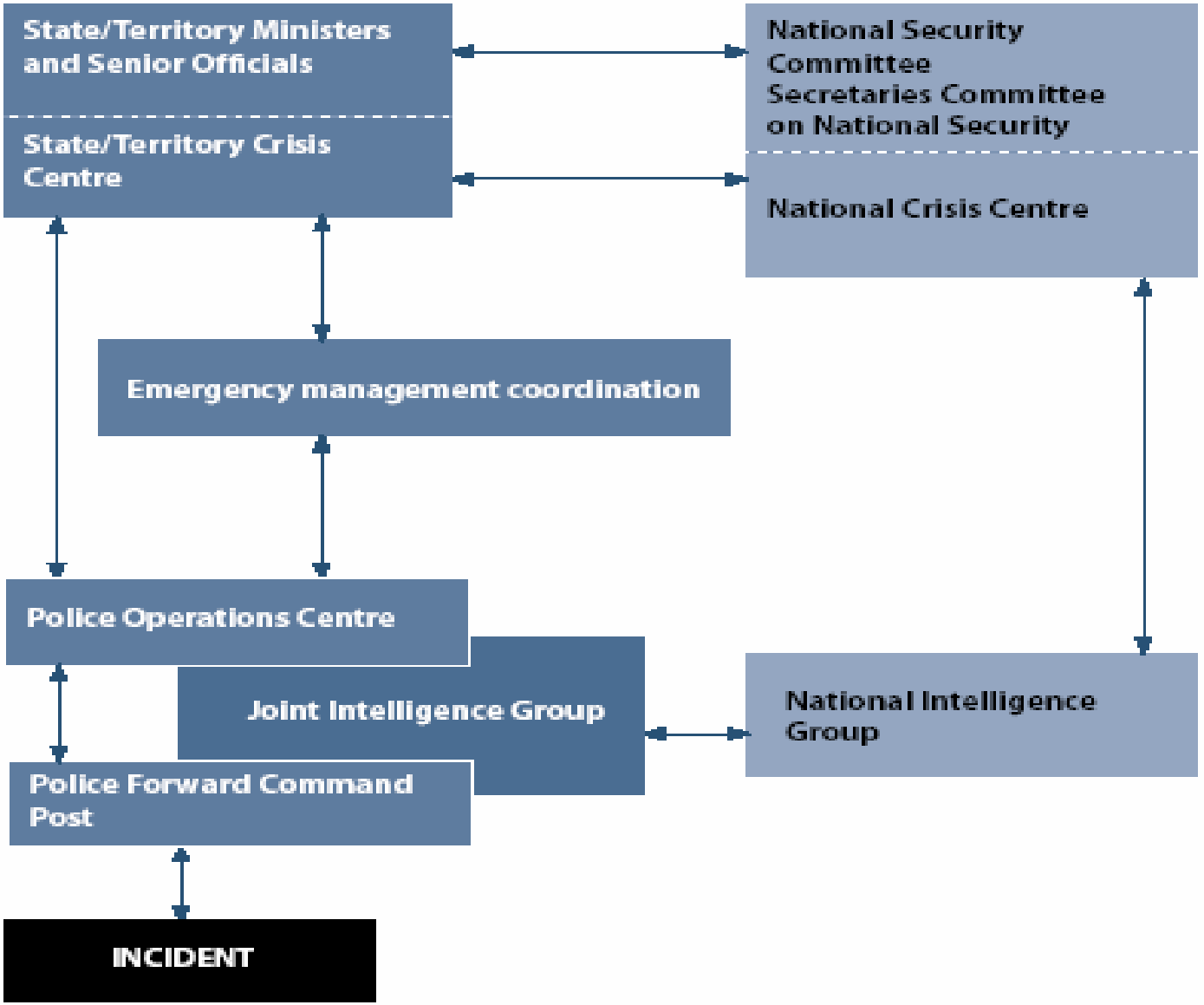
Pong Su Incident – Conclusion

- The operations surrounding the seizure of the Pong Su were seen as an unprecedented success.
- It was an operation dominated mostly by technical interoperability in that a well defined task was presented to all participants.
- However, further improvements in technical interoperability might have been achieved if the appropriate information systems had been more widely used.

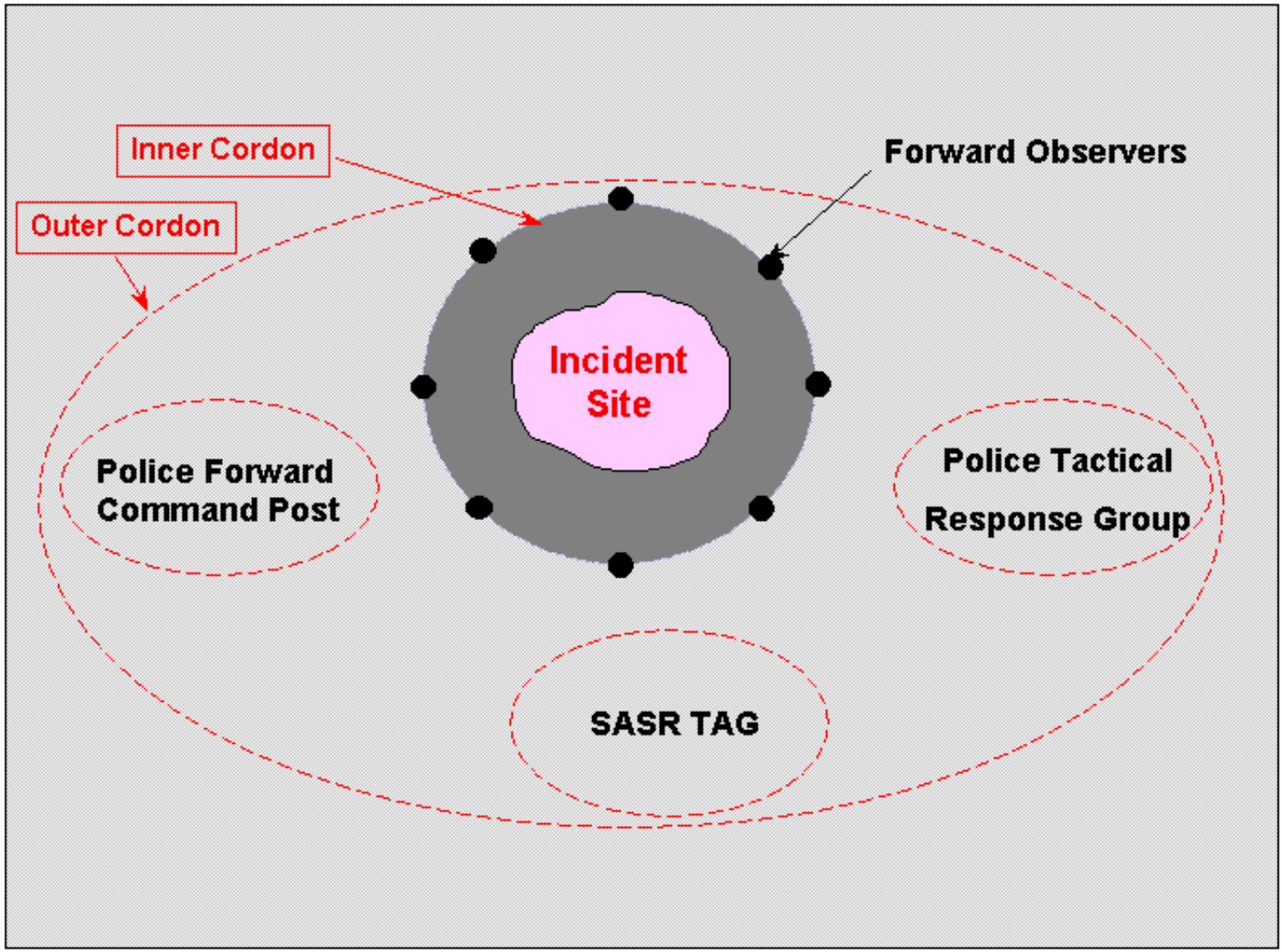
CT Exercises in Australia

- Counter Terrorism exercises are part of the Australian Government approach to emphasise the importance of being prepared for such incidents and demonstrate high-level commitment from Federal and State and Territory counter-terrorism agencies with a role in security, law enforcement, intelligence and emergency management
- The organisation of counter terrorism forces for Australia is detailed within the National Counter-Terrorism Plan published by the National Counter Terrorism Committee Organisation at an incident.
- The important aspect of this is that the Police remain in control and not the contingent from Defence once the SASR Tag is called out.

CT Exercises in Australia – Management Arrangements



CT Exercises in Australia – Management Arrangements



- A large degree of organisational interoperability exists and this is clearly detailed in the National Counter Terrorism Plan.
- Technical interoperability, however, appears to be less well served, with only ASNET providing some level of information exchange, probably at the strategic and operational level for intelligence.
- It is unclear whether tactical intelligence could flow in the time scale required over ASNET or whether any operational data would flow over ASNET.

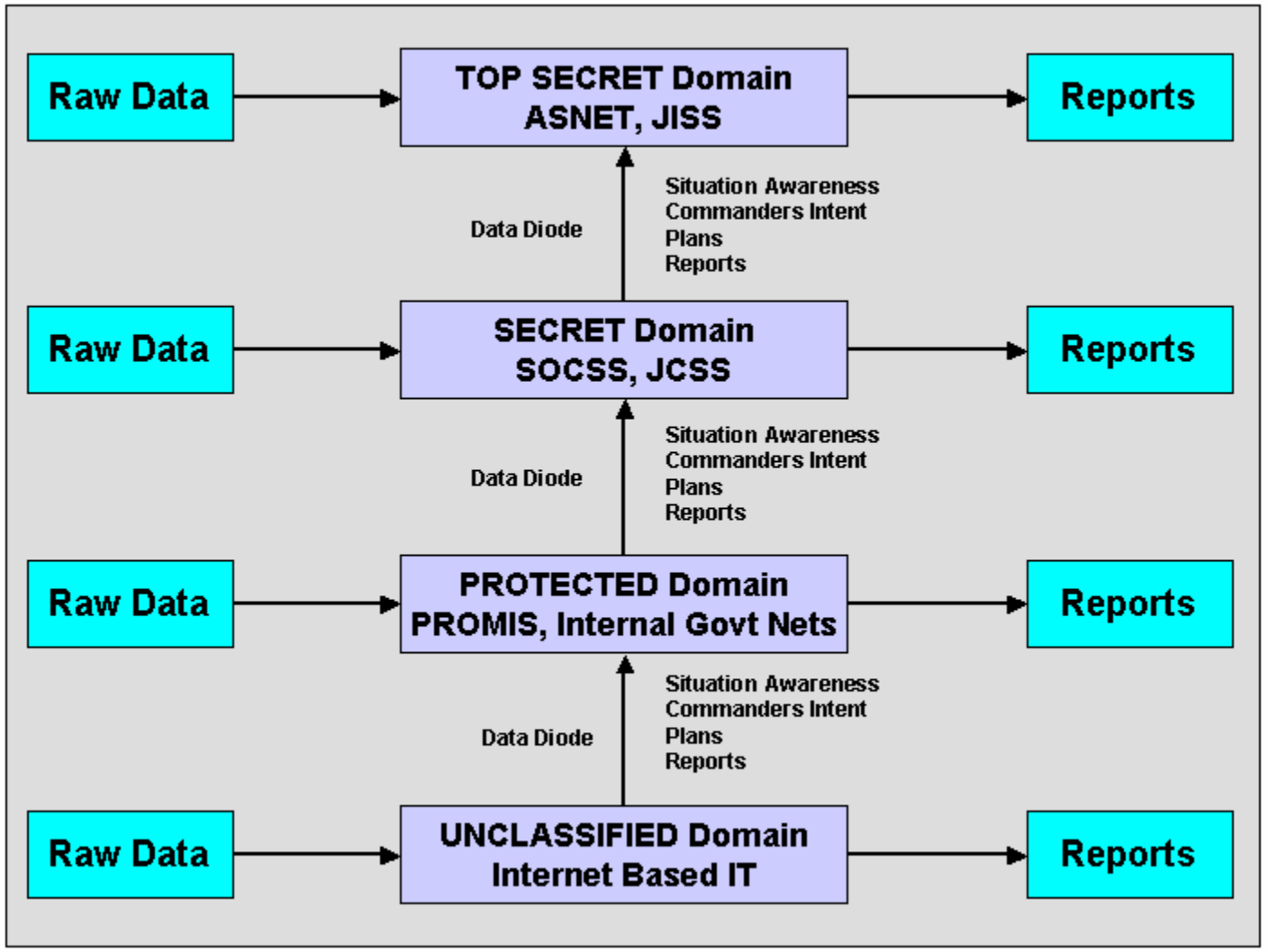
Lessons Learnt from Case Studies

- From and examination of the above case studies, the greatest deficiency in achieving technical interoperability is the lack of interoperability of tactical communications systems, especially radio networks.
- The case studies show that organisation interoperability could only be established if there were some basis for common organisation, procedures and actions amongst organisations.
- To improve organisational interoperability, efforts should be made throughout government, both state and federal levels, to establish a common security classification system.

Security Issues

- The key issue that emerges is that of security. It is also an issue in which both technical and organisational interoperability must be addressed in concert. New principles need to be established and agreed to allow the exchange of classified information.
- The requirement for “need to know” in all jurisdictions works against the “all informed” concept with most information systems.
- Operational interoperability could be addressed through the implementation of a **security architecture**. Such a security architecture needs to be segmented into at least four security domains to protect information correctly within the system.

Security Issues - Architecture



Conclusion

- Operational interoperability, because it embodies the established operating procedure of each organisation cannot be achieved during an incident, it must be addressed and solved prior to any operation involving multiple agencies
- Technical interoperability requirements are easier to define and are also easier to achieve in incidents that have relatively few objectives, even when a number of agencies are involved
- Technical interoperability issues in regard to security can be easily solved; however, organisational interoperability will require significant effort and the development of a security architecture for this purpose is proposed

Conclusion

- Case studies have shown the within the Australian context, that whole of government interoperability does not yet exist for either organisational or technical interoperability
- A key issue in achieving whole of government interoperability is security.
- Technical interoperability issues in regard to security can be easily solved; however, organisational interoperability will require significant effort and the development of a security architecture for this purpose is proposed.

Questions

ADI