4

Interoperability

4.1 In his National Security Statement to the Parliament of Australia the then Prime Minister of Australia the Hon. Kevin Rudd MP stated that:

> I believe that Australia's national security community is highly effective and has proven highly adaptable. But in an increasingly complex and interconnected security environment, we need a more integrated national security structure that enhances national security policy coordination.[1]

4.2 Following this statement the Counter-Terrorism White Paper stated that:

> Australia's counter-terrorism efforts are intelligence-led and focused on prevention. This approach hinges on strong partnerships and cooperation at the national level, effective engagement at the international level, and effective information sharing. Over recent years, there has been significant growth in Australia's security, intelligence and law enforcement agencies and the Government has taken steps to improve their capabilities and enhance information sharing. The establishment of the National Intelligence Coordination Committee has ensured that Australia's intelligence effort, both domestically and internationally, is better integrated into the new national security arrangements. The creation of a new Counter-Terrorism Control Centre will also ensure that we better integrate our overall counter-terrorism intelligence capabilities.[2]

---

1 The Hon Kevin Rudd MP, *First National Security Statement to the Parliament*, Department of the Prime Minister and Cabinet, Canberra, 4 December 2008, viewed on 19 April 2011, <http://pmrudd.archive.dpmc.gov.au/node/5424>.

2 *Counter-Terrorism White Paper, Securing Australia, Protecting Our Community,* Department of the Prime Minister and Cabinet, Canberra, February 2010, viewed on 19 April 2011, <http://www.dpmc.gov.au/publications/counter_terrorism/exec_summary.cfm>.

4.3 Given these statements the Committee thought it timely to ask that the AIC report to it on issues of interoperability.

4.4 The Committee asked that a separate section of each of the AIC agencies submissions address some or all of the following:

- Areas of interoperability between the AIC and any other Department or Agency;
- Any e-security arrangements underpinning this interoperability;
- Memorandum of Understandings providing the basis for interoperability;
- Accommodation requirements;
- Public relations and/or public reporting requirements as result of interoperability arrangements;
- Direction and strategic planning underpinning interoperability;
- How interoperability is being managed administratively;
- How interoperability is being managed financially;
- The effects of interoperability on performance management and evaluation;
- The effects of interoperability on recruitment and training; and
- Costs and benefit analysis of interoperability.

4.5 All of the agencies included information on interoperability in their submissions to the Committee. Given that issues relating to interoperability go directly to the operational priorities and practices of the agencies evidence to the Committee on interoperability is overwhelmingly classified SECRET and cannot be referred to in this report.

4.6 The Committee therefore outlines some of the publicly reportable information on the interoperability of the AIC.

The National Intelligence Coordination Committee

4.7 The National Intelligence Coordination Committee (NICC) is chaired by the National Security Adviser and comprises the heads of the Office of National Assessments, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate, the AFP, the Australian Crime Commission, and Customs and Border Protection. The departments of Defence, Foreign Affairs and Trade, Immigration and Citizenship, and Attorney-General's are also represented at the Deputy Secretary level.

4.8 The NICC enhances the ability of Australia's security agencies to share information, coordinate effort and identify opportunities to improve the whole-of-government response to terrorism and other national security challenges.

4.9 The NICC oversees the operations of two sub-committees: the National Intelligence Collection Management Committee (NICMC) and the National Intelligence Open Source Committee (NIOSC). Both of these committees are chaired by ONA.

The National Intelligence Collection Management Committee

4.10 The NICMC is responsible for setting specific requirements and evaluating collection effort against each of the National Intelligence Priorities set by the government.

The National Intelligence Open Source Committee

4.11 The NIOSC is responsible for enhancing the coordination and capabilities of the National Intelligence Community's open source efforts. Open source collection is considered the first information source for meeting the government's intelligence and security requirements.

The National Threat Assessment Centre

4.12 The multi-agency National Threat Assessment Centre (NTAC) is located within ASIO and assesses intelligence and information from a wide range of sources to prepare threat assessments in relation to specific people, places, and events. These assessments inform the risk management decisions made by operational agencies, the implementation of protective security measures and the travel advisories regarding potential threats when travelling overseas that are prepared by the Department of Foreign Affairs and Trade for the Australian public. ASIO also provides protective security advice to Australian Government agencies and, with the approval of the Attorney-General, to state and territory governments and private sector companies to protect vulnerable facilities.

National Interception Technical Assistance Centre

4.13 ASIO gave evidence to the Committee that it is working in partnership with the AFP and other Commonwealth agencies to provide coordinated technical assistance to other Australian intercepting agencies.

4.14 In 2010-11 ASIO will conduct a pilot study for the establishment of a National Interception Technical Assistance Centre (NiTAC). The NiTAC is planned to provide a central point of reference from which agencies can receive technical assistance to help keep pace with the rate and scale of technical change.

The Cyber Security Operations Centre

4.15 The Cyber Security Operations Centre (CSOC) is a Defence Signals Directorate capability that serves all government agencies.

4.16 The CSOC has two main roles:

- it provides government with a comprehensive understanding of cyber threats against Australian interests; and
- it coordinates operational responses to cyber events of national importance across government and critical infrastructure.

4.17 The CSOC serves all government agencies and has embedded representation from a number of other agencies involved in assessing the threat to, and the protection of, Australian interests from sophisticated threat actors. The CSOC will also assist CERT Australia[3], in the Attorney-General's Department, to support industry that owns or manages critical infrastructure.

Conclusions

4.18 The Committee was pleased with the level of information given to it in relation to interoperability and will continue to monitor this area to ensure that interoperability management and budgetary structures are in place across the AIC.

3 Australia's official national computer emergency response team.