7

Other Issues

7.1 During the course of the Review, a number of other issues were covered that did not fit into the broad subject areas the Committee resolved to examine during its consideration of the *Defence Annual Report 2012–13*. This chapter will consider these issues.

7.2 These issues are:

- Accounts Management; and
- Cyber-Security

Accounts management

Transaction processing

7.3 The Committee requested information on account management and transaction processing, particularly in regards to credit cards issued by the Department.

7.4 Defence told the Committee that its credit card centre in Hobart manages approximately 67,000 travel credit cards and 6,000 purchasing credit cards which are used to purchase items used in the regular day-to-day operations of the Department. In total, Defence manages approximately 70 per cent of all credit cards issued across the Commonwealth.[1]

7.5 Defence provided further information on the credit card centre in Hobart:

> A staff of about 15 people manage those credit cards…Their roles include issuing credit cards, the following up of lost and

[1] Mr Prior, Department of Defence, *Transcript*, 6 June 2014, p. 60.

> misplaced credit cards for our staff… and dealing directly with credit card companies in terms of transaction files.[2]

7.6 The Committee was interested to hear if there was any scope for interagency rationalisation in terms of managing Commonwealth issued credit cards. Given Defence already manages 70 per cent of all credit cards issue, the Committee enquired whether Defence should be taking a lead role in this area.

7.7 Defence responded by acknowledging that the Commission of Audit has made several recommendations on this topic which are currently being followed up the Department of Finance. However, Defence felt that it was not in a position to comment on the roles of other Government agencies in their management of credit card accounts and transactions.[3]

7.8 Defence reaffirmed that any future attempts to centralise the Government's interagency management of credit cards falls is still subject to the Commission of Audit.[4]

Cyber-Security

7.9 One issue brought to the Committee's attention was the lack of detail within the *Defence Annual Report 2012–13* dedicated to the issues of cyber-security in Australia.

7.10 In their submission, QinetiQ Australia stated that there are three particular areas in the realm of cyber-security that need to be considered by Defence:

- A need to understand the overlap between cyber issues and conventional military operations;
- A need to recognise that the cyber-domain crosses the civil-military boundary in the same way it crosses conventional military domain boundaries; and
- Recognise the human element in cyber security.[5]

7.11 Representatives from QinetiQ Australia clarified their point on the human element within cyber security during the public hearing:

> I believe there is much more to be done in recognising the vulnerability to cyber-attack, especially from insider threat… There is much that industry can do in this human factors domain

[2] Mr Prior, Department of Defence, *Transcript*, 6 June 2014, p. 60.

[3] Mr Prior, Department of Defence, *Transcript*, 6 June 2014, p. 61.

[4] Mr Richardson, Department of Defence, *Transcript*, 6 June 2014, p. 61.

[5] QinetiQ Australia, *Submission No. 2*, p. 6.

> including working jointly with the department and academia to address the identification of risk factors, potential risk behaviours and to height security cultures through psychology and sociology research, training and monitoring.[6]

7.12 The Committee asked for QinetiQ Australia's opinion on the level of competency exhibited by the Australian Defence Force (ADF) in terms of understanding the link between cyber issues and conventional military operations.

7.13 QinetiQ clarified their point by stating that the ADF tends to focus its resources on its defensive posture as opposed to using its resources to encourage the commercial sector and academia to address home defence issues:

> I am delighted to see and, indeed, be a part of DSTO's very strong new focus on research associated with cyber-warfare and cyber-defence…The area I have been pushing for within that with the Chief Defence Scientist and his team is to make sure that research does not just look at the 0s and 1s – the technology – but also looks at the human factor aspect as well.[7]

7.14 Drawing from their own experience, QinetiQ Australia informed the Committee that the United Kingdom announced plans in 2013 to establish a "Joint Cyber Reserve" in order to maintain a standing work-force of technical expertise available to the British Ministry of Defence. QinetiQ recommends the need for a similar body in Australia.[8]

Committee comment

7.15 The Committee acknowledges the growing significance of cyber-security as a new frontier for Defence. While cyber connectivity has generated significant technological advancements, the Committee is aware that this will continue to present new challenges for Australia's security environment.

[6] Mr Woolford, QinetiQ Australia, *Transcript*, 6 June 2014, p. 10.

[7] Mr Woolford, QinetiQ Australia, *Transcript*, 6 June 2014, p. 13.

[8] QinetiQ Australia, *Submission No. 2*, p. 7.

Recommendation 8

The Committee recommends that Defence Annual Reports include appropriately detailed information on the direction and development of the Department's cyber-security capabilities.

Senator David Fawcett
Chair
Defence Sub-Committee

The Hon Teresa Gambaro MP
Chair
Joint Standing Committee on Foreign Affairs, Defence and Trade