DEFENCE SUBMISSION TO JOINT STANDING COMMITTEE ON FOREIGN AFFAIRS, DEFENCE AND TRADE INQUIRY INTO THE DEFENCE ANNUAL REPORT 2007-08

PROLIFERATION SECURITY INITIATIVE

Defence's participation in the Proliferation Security Initiative (PSI), (a "means of cooperating to prevent illicit trafficking in weapons of mass destruction") and regional counter proliferation engagements, as well as training, preparation and response to radiological threats. PSI entails signing up to the Statement of Interdiction Principles (SIP), and participation in training and exercises. 'More than 90' countries are involved (DFAT).

1. What is Defence's assessment of levels of risk from Weapons of Mass Destruction for Australia and the region? What levels of risk are anticipated for the future?
The proliferation of Weapons of Mass Destruction (WMD) is, and will likely remain, a security issue of concern to Australia. The number of states with WMD, or with a 'break out' capability to rapidly produce WMD, is growing due to increasing industrialisation in the region. Moreover, terrorist groups have expressed a desire to acquire WMD. Proliferation networks have, in the past, been active in the region, and inadequate export controls means that the region is likely to remain attractive to proliferators. Law enforcement, counter-proliferation and export control regimes, and security assurances up to and including US extended deterrence will likely remain features of the region's response to such risks.

2. Can you give the Committee further detail on/about Australia's involvement and obligations under PSI? To what extent is Defence involved in fulfilling Australia's PSI obligations?
Australia has continued its strong involvement in, and support for the PSI since its inception by the United States in 2003. The PSI creates a framework for practical international cooperation to combat the illicit transfer of WMD, delivery systems and related materials. PSI participants endorse the 'Statement of Interdiction Principles', which aims to build upon participants' existing defence, enforcement, intelligence and diplomatic capabilities consistent with domestic and international law – to deter, interrupt and interdict the transhipment of WMD materials.

Through the Statement of Interdiction Principles, participants commit to:

- Undertake effective measures, either alone or in concert with other states, for interdicting the transfer or transport of WMD, their delivery systems, and related materials to and from states and non-state actors of proliferation concern;
- Adopt streamlined procedures for rapid exchange of relevant information concerning suspected proliferation activity, protecting the confidential character of classified information provided by other states as part of this initiative, dedicate appropriate resources and efforts to interdiction operations and capabilities, and maximise coordination among participants in interdiction efforts;
- Review and work to strengthen their relevant national legal authorities where necessary to accomplish these objectives, and work to strengthen when necessary relevant international law and frameworks in appropriate ways to support these commitments;

- Take specific actions in support of interdiction efforts regarding cargoes of WMD, their delivery systems, or related materials, to the extent their national legal authorities permit and consistent with their obligations under international law and frameworks.

The PSI is now supported by 94 countries (as at April 2009) and PSI activities are coordinated by a 20-country Operational Experts Group (OEG), which includes Australia. Defence has operational responsibility for PSI issues, while DFAT has policy responsibility, and a range of other Australian agencies contribute technical expertise.

On the occasion of the PSI's fifth anniversary, the United States hosted a senior-level meeting of PSI-endorsing countries in Washington (28 May 2008). The meeting set broad strategic directions for the PSI including a stronger focus on strengthening and widening support for the PSI in key regions, including the Asia-Pacific. Australia attended the meeting and, in concert with PSI partners, continues to support the implementation of the new strategic directions. These efforts include practical, operational support for the PSI in the region, participation in regional PSI exercises (eg New Zealand's PSI Exercise Maru in September 2008), and related regional outreach on the PSI.

3. How involved is Defence in PSI? Can Defence tell the Committee of instances where the PSI *Interdiction Principles* have come into play? Do PSI scenarios emerge that are not covered by the *Interdiction Principles*?

Defence is actively involved in the PSI, including through annual international meetings of the OEG (the Australian delegation is led by Defence), workshops and multilateral exercises. Defence actively participates at these meetings and in exercises and conducts outreach education and workshops to encourage greater support for PSI from regional countries. Moreover, Defence has been extensively involved in all of the activities hosted by Australia including two OEG meetings (in 2003 and 2004) and two PSI exercises (in 2003 and 2007). Defence has supported PSI exercises in other Asia-Pacific countries (eg New Zealand, Singapore and Japan) with ships, aircraft and specialist personnel.

The Australian Defence Force (ADF) provides support to Australia's PSI activities through the provision of assets to PSI tasks, advice to the Government on PSI matters and liaison/training with other government departments and other nations supporting the PSI. The ADF undertakes PSI tasks at the request of the Australian Government and within the guidance provided by the 'Statement of Interdiction Principles'. While Defence cannot discuss specific PSI activities due to operational security, the ADF has been involved in PSI tasks. Tasks undertaken by the ADF were initially requested by other nations supporting the PSI initiative, with Australian Government endorsement.

A PSI scenario has not emerged – and is not anticipated to emerge – that is not covered by the PSI Statement of Interdiction Principles.

RADIOLOGICAL THREATS

4. What is Defence's assessment of the current and future levels of radiological threat for Australia and its region?
The Defence Intelligence Organisation (DIO) conducts classified intelligence assessments relevant to the defence of Australia and its interests. Domestic security is not part of DIO's mandate, but is the responsibility of agencies outside the Defence portfolio. DIO routinely provides assessments relating to Chemical, Biological, Radiological and Nuclear (CBRN) threats to the ADF, and in support of whole-of-government counter terrorism and counter proliferation efforts; but these are subject to national security classifications and are not available at the unclassified level.

5. Can you tell the Committee about levels of training and preparedness for radiological threats that fall under Defence's area of responsibility?
ADF personnel undertake familiarisation training in the areas of CBRN defence as part of Basic Training. Furthermore, some ADF groups undertake additional training based on their primary role and likely tasks. Unit CBRN Defence Advisers, qualified through the School of Military Engineering's CBRN Instructor/Adviser course, receive four days of training (per course) on radiological issues. Training covers a broad range of aspects concerning radiological threats. The School runs three courses per year. Selected officers attend the Advanced CBRN course in Canada. This course offers further instruction on providing radiological threat advice to operational planning and higher headquarters. Defence also conducts the Defence Ionising Radiation Safety Officers Course for specialist personnel from across Defence.

6. Are units of Defence routinely equipped, trained and exercised in anticipation of radiological threats?
As with all possible threats to Australia and its interests, Defence takes an holistic view and works closely with other Government agencies to put in place the necessary plans, specialist personnel, organisations and equipment to effectively deal with a radiological incident. The Incident Response Regiment is prepared to deal with CBRN threats and its collective training levels are considered high. Specialist equipment and training enable its personnel to deal with radiological threats. The need for specific training and exercising for a response to a radiological threat scenario is determined by the assessed threat. Unit CBRN Defence Advisers provide the ability for Defence to surge its training if dictated by an increased threat.

7. Where a radiological threat emerged, other arms of government would come into play. Which other services would be involved, and does Defence conduct regular exercises with these services with respect to radiological threat scenarios?
Should a radiological incident occur, a number of Australian agencies and organisations would be involved. These include Emergency Management Australia in the Attorney-General's Department and the Australian Nuclear Science and Technology Organisation. The duties and responsibilities of these organisations are articulated in the National Counter Terrorism Handbook, which is produced by the Attorney-General's Department but is not a publicly available document. Defence has raised the CBRN Directorate in the Vice Chief of the Defence Force Group that, among other things, is tasked to provide a conduit for working-level engagement between Defence, Commonwealth and State Governments on CBRN matters. This Directorate is coordinating the Defence participation in the upcoming Department of Foreign Affairs and Trade led Discussion Exercise 'Blue Glow', which will be held in

Canberra from 7-8 May 2009. The Incident Response Regiment conducts regular exercises with the other agencies and organisations.

8. Are there instances where this capability has been brought into play, either due to an anticipated or an actual radiological threat?
There is no recent history of an actual radiological threat response involving the ADF. On two separate occasions in the 1980s and one incident in 2001, Defence was requested to provide assistance to the Australian Nuclear Science and Technology Organisation in the unlikely event that damaged weather satellites entered the atmosphere and crashed into Australia. The satellites self-destructed as planned and Defence assistance was not required.

THE STATE OF PREPARATION WITHIN DEFENCE FOR OIL DEPLETION AND OIL SHOCKS

Over the last 40 years we have seen a number of instances where oil has suddenly become less available and consequently more expensive. There is also discussion over whether oil has reached, or will reach, a peak in terms of worldwide production. Both of these influences represent risk for an organisation, such as Defence, which relies on oil as an integral part of its business:

9. Can you tell the Committee what measures have been taken by Defence to mitigate these risks?
Fuel is a critical component of Defence capability as it provides the means by which the ADF is able to operate its military platforms. Defence is conscious of ongoing global pressures on oil production and the potential risks to securing a sustainable supply of fuel to support the ADF in certain emergency scenarios. Defence mitigates these risks through its involvement in the established national liquid fuel emergency response mechanism and its own internal fuel management planning.

The *Liquid Fuel Emergency Act 1984* (the Act) provides the legislative basis for managing liquid fuel emergencies in Australia. The Government has established the National Oil Supplies Emergency Committee which is the main executive mechanism by which the Commonwealth, State/Territory Governments and Australian industry develop national responses to fuel supply emergencies. Defence is a standing member of the National Oil Supplies Emergency Committee and contributes to liquid fuel emergency planning. A National Liquid Fuel Emergency Response Plan has been developed by the National Oil Supplies Emergency Committee and would be implemented during a national liquid fuel emergency. Such emergencies would be managed through a combination of government intervention and market responses.

Although Defence is a comparatively minor user of fuel within the broader national context, the importance of maintaining fuel supplies to the ADF is recognised by both legislation and the National Oil Supplies Emergency Committee. Consequently, there is a standing process for designating the ADF as a priority fuel user in a national fuel supply emergency. This includes:

- The Governor-General would declare a national liquid fuel emergency under the Act if a severe disruption to national fuel supplies existed.

- The Minister for Resources, Energy and Tourism would then be provided with wide-ranging powers to control the drawdown, transfer and sale of crude oil and liquid fuels. The Minister would also have the power to control bulk and retail sales across Australia.
- If the Act was invoked, Defence would seek from the Minister for Resources, Energy and Tourism identification as a 'bulk customer' under s.10 of the legislation. This would be provided to Defence given its role in facilitating a Government response to any emergency and would allow Defence to receive bulk deliveries of fuel from suppliers.
- Defence would also seek to be identified as an essential user under s.11 of the Act. Under the legislation, all organisations involved in activities related to the defence of Australia are considered essential users.
- The National Liquid Fuel Emergency Response Plan would be implemented. The National Oil Supplies Emergency Committee would ensure that all 'essential users', including Defence, had sufficient fuel to meet their requirements.

Although the Act provides a robust legislative mechanism to guarantee the supply of fuel for the ADF during national fuel emergencies, Defence is also strengthening its strategic management of fuel to ensure that it can effectively respond to issues such as escalating oil prices. Defence is focused on internal policy reform and strategic engagement to drive a comprehensive whole-of-Defence approach to fuel management. The Defence Fuel Management Committee has been re-established to provide a coordinated whole-of-Defence approach to fuel management and acts as the principal advisory body to the Chief of the Defence Force on fuel-related matters. The Committee has recently agreed to oversight the development of a Defence Fuel Strategy which, among other things, will consider measures aimed at enhancing Defence's responsiveness to future global oil trends.

During a major oil shock, Defence would review its fuel demand and usage requirements and only seek to procure fuel that was essential to operations. Defence maintains 'Stock on Hand' which could be used to mitigate against a short-term fuel shock. However, the circumstances surrounding the shock, likely period of fuel outage/shortage and consequent level of ADF intensity for the period of the fuel shortage would determine the endurance of the fuel held in bulk storage. Work has also commenced to determine the strategic fuel reserve stockholding requirements of the Services. Accordingly, it is expected that surge provisions will be included within new fuel procurement arrangements that will enable Defence to task its commercial suppliers to meet heightened operational usage requirements at short notice.

The Department of Resources, Energy and Tourism is the lead agency responsible for developing a national, whole-of-government approach to resolving Australia's future energy security challenges through its Energy White Paper process. Defence will continue to participate actively in this process.

10. Is Defence engaged in research on alternatives to oil, and can you update the Committee on current research on this by Defence in the US?

Defence has undertaken some initial investigations into the effects of alternative fuels on the ADF and will continue to examine this issue. It should also be noted that international military organisations, such as the United States Air Force and the United Kingdom Ministry of Defence are playing a significant role in promoting the uptake and commercialisation of alternative fuels and power generation (for example, gas/coal/biomass to liquids for aviation fuels). However, in general, these processes are being developed in the commercial arena.

The Defence Science and Technology Organisation (DSTO) is responsible for coordinating research and providing specialist scientific advice to Defence technical regulatory authorities and capability developers on the suitability of alternative fuels for Defence platforms. The DSTO recently completed a study to estimate the joint fuel demands for the Navy, Army and Air Force. The DSTO is a partner with the United States, the United Kingdom and Canada in a Study Group examining future military power and energy requirements and supplies to identify collaborative opportunities in the energy domain. The DSTO has also recently established a new long-term strategy which aims to generate and develop a Science and Technology capability for Defence to analyse current and projected energy requirements and trends, identify areas where technology insertion may optimise energy management and usage, and develop and field test new technologies. The Commonwealth Science and Industrial Research Organisation (CSIRO) is working with Australia's transport stakeholders through the Future Fuels Forum to identify sustainable future alternative fuel sources. As part of its new strategy, the DSTO will work closely with the CSIRO and other agencies to investigate the development and use of alternative fuels.

The United States has been trialling alternative fuels in the United States Air Force. The use of alternative fuels in aviation applications requires development of detailed specifications, supported by comprehensive testing and certification activities to ensure that airworthiness requirements are not compromised. The United States Air Force has a forward program for certifying the use of alternative fuels in specific fleets such as B52 and C-17. The ADF remains engaged with the United States military to support the exchange of relevant information that is developed in the United States certification programs. The exchange of this information will allow Defence to position itself to exploit the benefits of alternative aviation fuels as they are certified for use and become commercially available.

CLIMATE CHANGE

Efforts by Defence to monitor and reduce its carbon footprint, to reduce ozone depleting substances and synthetic greenhouse gases.

11. Can you tell the Committee what Defence is doing to monitor its carbon footprint?
The task of defining the overall carbon footprint for Defence (including such complex aspects as whole-of-life assessments of resource inputs, use of resources, infrastructure and capability development, contractor inputs and operations in Australia and overseas), would be cost and resource prohibitive. Rather, Defence has approached the task by utilising the Whole of Government Energy Reporting regime as the method to monitor Defence's carbon footprint.

Defence reports on its greenhouse gas emissions from electricity, gas and operational fuel annually as part of the energy report regime to meet the Commonwealth Governments Energy Efficiency in Government Operations Policy (2006). The Department of the Environment, Water, Heritage and the Arts converts this energy use data into an estimate of greenhouse gas emissions using the methodology outlined in National Greenhouse Accounts Factors 2008 workbook which is produced by the Department of Climate Change.

12. Can you tell the Committee what Defence is doing to reduce its carbon footprint?
Electricity consumption is one of the main contributors to greenhouse gas emissions. As stated in the Energy Use in Government Operations report 2006-07, Defence is the largest consumer of electricity within the Commonwealth Government.

Defence is working to reduce energy consumption by increasing efficiency of existing equipment and infrastructure, for example by adjusting temperature control settings in buildings and replacing high energy using equipment with more efficient equipment. Defence is implementing a wide range of energy saving initiatives across the estate including Defence's Green Building policies, pilot energy efficiency projects, and the ongoing development of regional and site energy action plans and communication and support tools.

13. What figures are available on this? Has Defence bench-marked its carbon footprint, and how does it rate with comparable organisations?
Information regarding Defence's energy consumption is reported in the Energy Use in the Australian Government's Operations report. In the 2006-07 reporting period, Defence's energy consumption was around 4 million GJ, which is equivalent to approximately 1.6 million tonnes of greenhouse gas emissions.

Defence exchanges information on energy management with United Kingdom and United States defence organisations but has not undertaken a formal benchmarking exercise.

14. Similarly, can you tell the Committee about Defence's monitoring and management of ozone depleting substances and synthetic greenhouse gases? Are there reporting mechanisms for this? How does Defence rate compared with comparable organisations?
Defence is in the process of finalising an Ozone Depleting and Synthetic Greenhouse Chemicals Manual. This provides the policy under which Defence will meet its obligations under the Vienna Convention for the Protection of the Ozone layer, the Montreal Protocol on Substances that Deplete the Ozone Layer and the United Nations Framework Convention on Climate Change.

Defence must comply with the *Ozone Protection and Synthetic Greenhouse Gas Management Act 1989* (the Act) and the Ozone Protection and Synthetic Greenhouse Gas Management Regulations 1995 (the Regulations). In accordance with the Act, the acquisition, possession or disposal of fire extinguishing agents which are deemed to be scheduled substances is regulated and appropriate permits, licences and exemptions are required to be obtained from the Department of Environment, Heritage and the Arts (DEWHA) or the agency appointed by DEWHA to administer the regulations on behalf of the Government. The agency appointed by DEWHA to administer these regulations is the Fire Protection Association of Australia.

Defence monitors its stockpile of ozone depleting substances and synthetic greenhouse gases by fortnightly leak detection and biannual weighing of cylinders. Defence's leak monitoring is conducted above the minimum regulatory requirement.

Defence holds the following permit/authorisation that is related to the possession and trading of halon and non-halon extinguishing agents. These are:

- Halon Special Permit. Required for the possession or trading of halons.

- National Extinguishing Agent Trading Authorization. Required for the acquisition, storage and disposal of bulk extinguishing agents that are scheduled substances.

Defence also hold a Refrigerant Trading Authorisation.

Up-to-date records showing the amounts of extinguishing agents and refrigerants acquired, disposed of and recovered from any source are to be reported to DEWHA or the above mentioned agency.

Defence's monitoring and reporting is comparable to other public sector organisations and meets regulatory requirements. Defence closely aligns its system of managing ozone depleting and synthetic greenhouse gases with DEWHA. A Memorandum of Understanding is currently being developed between the two departments. This agreement will formalise arrangements and bond common objectives of enhanced control and the uptake of alternatives as they become available.

Defence also works closely with the Australian Refrigeration Council and Fire Protection Association of Australia to ensure good regulatory control throughout the organisation.

15. Is there room for improvement on Defence's management of carbon, ozone depleting and synthetic greenhouse gases?

Defence takes an active interest in alternative monitoring strategies being developed by DEWHA.

Through Joint Logistic Command's Safety and Environment Section, Defence actively engages in discussion with international partners, such as the US Defense Department and Environmental Protection Agency to keep informed of advances in replacement technologies and regulatory reform, including those emanating from the Montreal Protocol's Technical Committees.

The replacement of ozone depleting substances and synthetic greenhouse gases with less hazardous extinguishing agents is under constant review. Defence has conducted trials of alternative fire extinguishing agents and hopes to participate in upcoming research projects with our US partners.

The search for ozone depleting substance alternatives will change the way Defence makes procurement decisions. Defence sources the majority of its equipment from other countries such as the United States, and is reliant on platform design changes in those countries to eliminate the use of ozone depleting substance. Defence recognises the need to become an influential and informed consumer and to carefully consider commercially viable replacements for ozone depleting substances. With a greater reliance on civilian systems and solutions, equipment selection will continue to be based on a rational assessment of value-for-money and fit-for-purpose requirements.

CYBER WARFARE

16. Can you tell the Committee about Defence's involvement with Cyber Warfare? What areas of activity is it pursuing, and which receive high priority?
All Internet-connected systems are potential targets for electronic attack so it is critical that Australia has an effective defensive capability.

The Chief Information Officer Group (CIOG) in the Department of Defence employs a wide range of measures to protect its networks from such threats and actively monitors its systems to detect potentially malicious activity. The Defence Network Operations Centre provides this capability and works closely with the Defence Signals Directorate (DSD) to ensure its measures are able to protect Defence information and systems in a dynamic threat environment.

DSD is pursuing areas of activity that will enhance its ability to discover and respond to threats to Government networks as well as improve our ability to identify vulnerabilities in those networks.

As DSD draws on classified capabilities and sources of information to meet Government security requirements, it does not publicly disclose the details of those capabilities.

17. There are celebrated cases where state and non-state actors have entered Defence secure networks in the US. Have similar events occurred in Australia? What measures are being taken by Defence in Australia to protect against such events?
While Defence does not comment on the security status of Defence information systems, the CIOG actively defends its systems from a range of cyber threats.

As the national authority on information security, DSD provides material, advice and assistance to Commonwealth and State/Territory authorities. This includes assisting the Defence CIOG with cyber threat detection and warning for Defence information systems.

DSD and CIOG have ties with close allies, and cooperate with relevant agencies. When such threats have arisen in our partners' countries, DSD and CIOG have been informed and DSD has provided technical advice and assistance to the CIOG to ensure the confidentiality of sensitive information and the integrity of its networks. DSD also performs detection and reporting on cyber threats to Government agencies; this includes a seven-day, 24-hour incident response capability.

18. The Committee is aware that the Network Centric Warfare capability is a primary focus for Defence. This is also potentially vulnerable to an opponent's cyber warfare capability. To what degree is Defence satisfied that it can protect its war-fighting networks against this kind of attack, and what specific mechanisms are in place to achieve this?
Implementation of the Network Centric Warfare concept in Defence and the ADF is a critical force multiplier and it is important that the systems that contribute to that goal are protected from all forms of attack. The targets of hostile cyber warfare activities of concern to Network Centric Warfare are the networks that carry the essential information and intelligence. The protection of these networks includes physical, personnel and information security measures in accordance with Government information security.

19. Given the centrality in Defence of IT-based data and communications networks, can you comment on the adequacy of resources and attention being applied to this area?
The Defence CIOG operates the Defence Network Operations Centre to provide comprehensive monitoring and response to cyber threats. It assigns resources in this area commensurate with the level of threat and the sensitivity of the information being protected.

Like all Government agencies, Defence CIOG benefits from DSD material, advice and assistance to protect its information systems. DSD has received funds to enhance its cyber defence capabilities under the E-Security National Agenda, approved in two tranches by the Government in 2001 and 2006. These enhancements focus on trialling a network monitoring capability, conducting vulnerability assessments and improving training and awareness of cyber threats and security measures across government.