Acknowledgments

The Office of the Inspector of Transport Security wishes to acknowledge the valuable input, advice, data and images received during this Inquiry. This includes from Australian Government, state and territory government agencies, international government agencies and domestic and international oil and gas industry companies and organisations. In particular, economic data and statistics contained in the Australian Oil and Gas Operations Section was provided by the Australian Petroleum Production and Exploration Association (APPEA) and the Bureau of Resource and Energy Economics.

With thanks for the images and charts provided by the following individuals and organisations:

Cover: Angel Platform, courtesy of Woodside Energy Limited.
Pg 1: Atwood Osprey, courtesy of Chevron Australia
Pg 7: Cobia Platform, courtesy of Esso Australia Pty Ltd
Pg 15: Slag Platform, courtesy of Apache Energy Limited
Pg 18: West Kingfish, courtesy of Esso Australia Pty Ltd
Pg 21: Atwood Osprey, courtesy of Chevron Australia
Pg 26: Karratha Gas Plant, courtesy of Woodside Energy Limited
Pg 58: offshore platform, courtesy of Esso Australia Pty Ltd
Pg 82: Maritime chart extract of chart Aus327 off Dampier, developed for the Inquiry by the RAN Australian Hydrographic Service
Pg 87: Maritime chart extract of chart Aus327 off Dampier, developed for the Inquiry by the RAN Australian Hydrographic Service
Pg 109: Ningaloo Vision, courtesy of Apache Energy Limited
Pg 111: North Rankin Platform, courtesy of Woodside Energy Australia
Pg 113: Varanus, Courtesy Apache Energy Limited
Pg 115: Atwood Osprey, courtesy of Chevron Australia
Pg 118: Pluto LNG, courtesy of Woodside Energy Australia
Pg 128: Pyrenees Venture, courtesy of Apache Energy Limited
Pg 131: Fortescue, courtesy of Esso Australia Pty Ltd

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Creative Commons licence

With the exception of (a) the Coat of Arms; and (b) the photos and graphics; copyright in this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.

Creative Commons Attribution 3.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

A summary of the licence terms is available from http://creativecommons.org/licenses/by/3.0/au/deed.en.
The full licence terms are available from http://creativecommons.org/licenses/by/3.0/au/legalcode.

This publication should be attributed in the following way: Offshore Oil and Gas Resources Sector Security Inquiry © Commonwealth of Australia 2012

© Commonwealth of Australia 2012
ISBN: 978-1-921769-72-6
June 2012 / INFRA1411
Email: publishing@infrastructure.gov.au
Website: www.infrastructure.gov.au
Contents

Executive Summary .............................................................................................................................. 1

   The industry position .................................................................................................................. 1

   The threat scenario ..................................................................................................................... 2

      On-site security audits and inspections .................................................................................. 3

      Active on-site exercises .......................................................................................................... 3

      Access and egress security ..................................................................................................... 4

      Security exclusion zones ......................................................................................................... 4

      Government and industry interaction and relationships ....................................................... 5

      Incident response—capacity, command and control ............................................................... 5

      Recruitment and vetting ......................................................................................................... 6

      Training and awareness ......................................................................................................... 6

Summary of recommendations and options for considerations .................................................... 7

   On-site security audits and inspections ..................................................................................... 7

   Active on-site exercises ............................................................................................................. 8

   Access and egress security ........................................................................................................ 8

   Security exclusion zones .......................................................................................................... 9

   Government and industry interaction and relationships ......................................................... 9

   Incident response—capacity, command and control ............................................................... 10

   Recruitment and vetting .......................................................................................................... 10

   Training and awareness ........................................................................................................... 11

   Cyber Security ......................................................................................................................... 12

   The US experience – possible approaches for Australia ............................................................ 13

   The North Sea experience – possible approaches for Australia ................................................ 13

   The Australian experience – possible approaches ................................................................. 14

Conduct of the inquiry ..................................................................................................................... 15

Introduction ..................................................................................................................................... 19

The legal framework ...................................................................................................................... 23

   International maritime law ....................................................................................................... 23

   Australian maritime law .......................................................................................................... 24

      Maritime Transport and Offshore Facilities Security Act 2003 .............................................. 25

International assessments ............................................................................................................. 29

   United States—Gulf of Mexico—oil and gas operations ............................................................ 29

   Agencies visited by the inquiry team ......................................................................................... 30

   Inquiry observations and options for Australia ....................................................................... 33
Australia is the world's ninth largest energy producer, accounting for around 2.4 per cent of world energy production. Australia produces coal, uranium, Liquefied Natural Gas (LNG), crude oil, Liquefied Petroleum Gas (LPG) and renewable energy. Oil and gas accounted for 17 per cent of Australia's total energy production in 2008–09.

Annually, Australia's oil and gas industries contribute 2.5 per cent of Australia's gross domestic product and generate $28 billion in revenue. In addition, they yield almost $9 billion in direct tax payments and contribute 58 per cent of Australia's primary energy needs.

While oil production is currently in decline in Australia, gas production is growing rapidly. LNG is widely recognised as a cleaner energy alternative to oil and coal for industrial and domestic use and worldwide demand is rapidly increasing, with production expected to rise by 50 per cent from 2011 levels to meet demand.

Current LNG projects, and those under development or consideration, exceed $200 billion in investment and, with long-term contracts and projected 25-year production fields, will contribute significantly to Australia's future economic wellbeing.

Consequently, the security and reliability of oil and gas production is becoming increasingly important. Of particular concern, are those oil and gas facilities operating offshore within Australia's Exclusive Economic Zone (EEZ).

Against this background, and consistent with the provisions of the Inspector of Transport Security Act 2006 (the Act), the current inquiry has focused primarily on assessing the state of affairs or matters that may reasonably be believed to have significant implications for security-regulated offshore facilities in general.

Although Australia can be confident that the security measures and practices in place generally reflect those in effect elsewhere, areas of vulnerability in current security-related practices and arrangements that warrant consideration and improvement have been identified through this Inquiry.

The industry position

The oil and gas industry is essentially risk averse and wants to operate in a secure offshore and onshore environment.

Offshore oil and gas exploration is expensive and risky and development and production require long-term planning and substantial investment.
The majority of oil and gas companies operating in Australian waters are multinational corporations with ventures in other parts of the world. As a result, company safety and security standards and practices tend to reflect a company’s international arrangements, tailored to reflect the perceived threats and risks in the location of operation.

While, understandably, the safety culture within the oil and gas industry is more entrenched and mature than that of security, companies are continually improving their security arrangements and practices. In places such as Africa and the Middle East, security arrangements are especially well developed and, in a number of cases, these arrangements have been actively tested.

Within the Australian environment, security planning is a relatively new priority with Australian-based management positions in company security being only reasonably recently introduced. A number of companies have tailored their international safety and security policies to meet Australian requirements and to the identified threats and risks.

While the larger companies are likely to have well developed security regimes in place, others, with less international or operational experience or with economy-of-scale restrictions, may have less rigorous and comprehensive security programs and face more difficulties in implementing a comprehensive security regime. As a result, the standard of security awareness and preparedness across Australian oil and gas operations is currently variable and will benefit from ongoing engagement with government.

The threat scenario

To date, Australia has been consistently considered as a low-risk, location with high security and supply reliability. However, the shape of the oil and gas industry is changing and Australia increasingly has a range of characteristics within its operating environment that are likely to heighten security implications in the future.

As the Australian-based industry and associated employment demands continue to grow, the employee profile of many companies is changing and more foreign workers, generally operating under 457 visa arrangements, are being engaged.

As is the case internationally, the ability to effectively vet potential employees, either through company recruitment processes, Maritime Security Identification Cards (MSICs), passport or 457 visa related checks is essentially limited to basic character style assessment and cannot operate as a genuine security clearance process. These limitations need to be understood and reflected in other and wider complementary security arrangements.

While there is no evidence, apart from the issue of cyber intrusion, of any specific threat against offshore oil and gas infrastructure in Australian waters, there is international recognition that threats to offshore infrastructure do exist. Terrorist groups have indicated an interest in economic targets, including oil and gas tankers and energy-related facilities, and United States of America (US) government authorities have identified that the petroleum industry may be a terrorist target due to the inherent nature of the business and the importance of the industry to the national interest. This assessment has obvious application to Australia.

In terrorist terms, international and Australian assessments indicate that the threat to offshore infrastructure could emanate from home-grown or internationally driven terrorist operations.
However, based on both government and industry advice and assessment, the risk of terrorist takeover of an offshore facility operating in Australian waters is low, with the much more likely threat seen as being caused by a ‘trusted’ or disgruntled insider or a lone perpetrator.

While in comparative terms Australian industry practices and Australian government/industry relationships generally reflect those practices and arrangements in place in other countries, terrorist and criminal groups (including determined lone perpetrators) have continued to demonstrate their adaptability, resourcefulness and capacity to find unexpected and unpredicted ways to breach security and cause harm and damage.

In terms of insider or intruder based threats, the tragic criminal attacks, allegedly committed by Anders Breivik in Norway on 22 July 2011, provide a dramatic example of the potential of an organised disaffected or unbalanced lone perpetrator. Breivik, apparently operating alone, has admitted carrying out two violent attacks in quick succession against the government, the civilian population and young Norwegians attending a labour party summer camp on Útøya Island near Oslo.

Against this background a range of vulnerabilities in the current Australian security framework, were identified that warrant specific examination. These are summarised below.

### On-site security audits and inspections

While all oil or gas offshore production facilities in Australia are required to have an approved offshore facility security plan in operation, the plans, in accordance with the current risk-based intelligence-led approach to security oversight, are only subject to desktop assessment and review as part of the approval process.

Although the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) conduct periodic on-site safety audits and inspections, it is understood no on-site offshore facility security assessments have been conducted since 2007.

Most companies do conduct their own internal security audits, but in most cases the facility security plans have never been subject to any independent external assessment and have not been tested by either active third-party audit or on-site exercising.

In the US Gulf of Mexico and North Sea environments, despite the quite different regulatory and oversight arrangements that have been implemented in each region, offshore facilities are subject to inspection and audit oversight.

In the opinion of the Inquiry, the current Australian situation is unsatisfactory and arrangements should be implemented which provide the capacity for an effective offshore security audit program to be introduced and maintained.

### Active on-site exercises

While within Victoria and Western Australia relevant state police engage on a regular basis in joint exercises with industry on near-shore offshore facilities, it is understood that no Commonwealth agency has participated in such exercises since about 2004.

Although the reasons are well known and understood, Australian Defence Force (ADF) exercises on or in the vicinity of offshore facilities, as occurred in the Bass Strait during the 1980’s, have rarely been conducted in recent years, either in Bass Strait or in Australia’s North West Shelf (NWS) region.
The Inquiry has been advised, however, that this issue is currently being addressed by the ADF as additional resources become available and discussions are already occurring between the ADF and NWS oil and gas companies with regard to the commencement of an exercise program in northern Western Australia.

Industry has expressed a willingness to assist government agencies, including particularly the ADF, to improve their understanding of offshore facility operations and the relevant security implications, by facilitating on-site visitations and short-term deployments of selected officers. The ADF has already expressed an interest in this proposal.

**Access and egress security**

Access and egress security, particularly at heliports servicing offshore facilities, is an area of concern. While the number of heliports currently servicing offshore infrastructure is low (currently less than 10), the current variations in security screening practices will benefit from review and regularisation.

Heliports servicing the offshore oil and gas industry have a variety of security arrangements in place to meet government regulation and operator requirements. Some heliports operate from within Aviation Transport Security Act 2004 (ATSA) regulated airports. As they are not involved in Regular Passenger Transport (RPT) aviation activities, they operate from separate general-aviation aircraft aprons and are not subject to any regulatory screening of passengers, baggage and stores carried by helicopters.

Helicopter operations servicing offshore facilities are required to have an approved maritime or offshore facility service provider security plan under the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA). However, if they are operating from private airports, neither the helicopter operations nor the private airports from which they are operating, are subject to ATSA security regulation.

As a consequence, airlines and helicopter operators contracted to offshore operators only provide the level of security and safety detailed under their contract. If specific security requirements such as screening of personnel, baggage and freight are not included in the contract then it is not likely to be provided. Similarly, where the offshore operator provides the operator’s own security regime this can vary from full screening of passengers, baggage and freight to minimal identity checking. These inconsistencies, and the ways by which they may be remedied or improved, are examined within this report.

**Security exclusion zones**

The current internationally agreed 500 metres security exclusion zone arrangements, which are in place around offshore production facilities, are considered by all industry stakeholders as too small and ineffective. Breaches of the zone have been demonstrated to be largely unenforceable and the 500 metres distance is too short to provide a facility operator with any realistic opportunity to implement defensive or evacuation strategies. A large fixed-production platform will usually take a minimum of 30 minutes to evacuate once a general alarm has been sounded. A vessel travelling at 20 knots will cover about 10 nautical miles in that time.

In many cases, exploration and production activities are conducted jointly by several companies in ventures that may involve a number of facilities grouped and linked within a reasonably small area. The current 500 metres security exclusion zone limits, which unlike safety zones, do not encompass hubs, pipelines and other linked infrastructure within their boundaries, are particularly ineffectual in these circumstances and are a point of vulnerability.
Consideration is given in this report to the ways in which the current 500 metres security exclusion zone limit could be replaced by a graded multi-layered security zone approach, which would provide more effective protection.

**Government and industry interaction and relationships**

Industry has emphasised the constructive relationship it generally enjoys with government agencies. There is, however, common agreement that increased engagement between industry and government security agencies, aimed at enhancing mutual levels of understanding - industries' knowledge of the intelligence gathering, analysis and dissemination processes of government and government's knowledge and expertise of industry - in the security space, is necessary.

While this initiative will make a positive contribution to the improvement of the nature and quality of intelligence sharing and the interaction between government and industry, the broader current levels of engagement and communication would benefit from further and ongoing improvement.

The Australian Security Intelligence Organisation (ASIO), which was already playing a constructive role in government and industry relationships through the publications of the Business Liaison Unit (BLU), have been quick to recognise and react to these industry concerns and an industry roundtable was convened by them in Canberra during March 2012 to specifically address the primary matters of concern.

**Incident response—capacity, command and control**

As mentioned previously, industry is concerned by the uncertainty that surrounds the response they may expect from government agencies to a serious security incident on an offshore facility. While the realities of isolation, distance, weather conditions, unpredictability and competing government priorities and responsibilities are understood by industry, there does appear to be a lack of clarity and an absence of a response framework sufficient to provide industry with reasonable confidence and comfort.

In any major safety or security incident, the first response of an offshore operator will be, in almost all circumstances, to shutdown the facility and evacuate all personnel. In such circumstances, it will be important for an offshore facility operator to have the clearest possible understanding of the nature and speed of response that could be reasonably expected from government agencies.

A related issue of concern to industry surrounds the current incident reporting arrangements. Reporting criteria are unclear and neither government agencies nor industry representatives appear to have a good understanding of initial point of reporting arrangements. Currently, there are multiple federal and state or territory reporting points, with the decision as to the agency to which a report should be made largely dependent on the nature of the incident.

Oil and gas companies have well-tested operational relationships with their relevant state or territory police service which, in many situations will be the immediate contact point and first responders to a security incident, but the situation is not as clear within the federal environment. While Border Protection Command (BPC) is the first federal point of contact for any maritime security incident, the situation may be different if the cause of the incident is accidental, unknown or undetermined.

The Inquiry is of the view that current federal reporting arrangements should be reviewed, with consideration given to the establishment of a single, triple-zero (000) style, federal contact point or centre for all incident and compliance related reporting situations.
The arrangements determining who the lead agency is and who has the command and control for incident management, particularly where the cause of an incident is not immediately known or is clearly simply a criminal matter rather than a terrorist incident, has also been identified as an issue of concern. Neither industry nor government agency representatives appear confident as to what arrangements would apply in a range of given situations. These uncertainties need to be resolved as a matter of some urgency and are examined in this report.

Recruitment and vetting
The vetting of Australian employees as part of the application process for a MSIC generally comprises a criminal-record check, as well as internal company checks deemed appropriate. Industry sees the MSIC process as providing an additional layer of security vetting above the level they can provide themselves. However, although the MISC vetting process provides a security assessment and a photographic record of an individual employee, the process is limited. Currently, the requirement for a MSIC does not apply to foreign nationals or to Australian and other workers engaged on non-regulated vessels operating under subcontract arrangements.

Companies are increasingly recruiting personnel from overseas due to skill shortages in Australia. Usually, these employees are granted a 457 visa (for professional and skilled migrants), which, again, involves only limited security vetting.

The above employee vetting limitations need to be understood (both by industry and government) in the development and maintenance of an overall, integrated security management system and are further examined in this report.

Training and awareness
Currently, the only endorsed training programs on security awareness that are in place for the offshore environment are those for company security officers and for ship or facility security officers. These courses are assessed and endorsed by the Office of Transport Security (OTS) and the Australian Maritime Safety Authority (AMSA), as appropriate, but are not currently subject to any formal accreditation.

Accredited training courses, to Certificate II or III standard, are required for maritime security guards and onshore perimeter or site security personnel, but the standards are inconsistent and, in some areas deficient. In particular, the Inquiry noted that some security guards were not conversant with the testing and use of screening equipment and their powers as a Maritime Security Guard (MSG) under MTOFSA.

There is no broader industry-wide, accredited security training program, nor are there security induction or awareness courses that are suitable to be delivered to new offshore or onshore facility employees. Any such awareness programs are conducted voluntarily and solely at the discretion of an individual company or operator.

The Inquiry found that onshore security-awareness training in Australia varied between companies and between facilities in the same company. Training ranged from a security-awareness component within site-induction programs for employees and visitors to little or no training at all.

The current situation and the steps that may be taken to improve the quality and consistency of relevant security training programs are examined in some detail in this report.
On-site security audits and inspections

1. RECOMMENDATION

The Inquiry recommends that the Australian Government enhance the current security compliance arrangements by implementing a formal offshore oil and gas production facility on-site audit and inspection program sufficient to confirm the quality and adequacy of security measures and the levels of understanding required by an offshore facility security plan.

POSSIBLE OPTIONS

1.1 Provide a single agency with the authority to conduct combined safety and security audits under the umbrella of an holistic ‘all-hazards’ approach to the maintenance of a safe and secure operational environment and adequately resourced to effectively perform the combined role.

1.2 Retain the current separation between safety and security audits and inspections, and equip the agency given the responsibility for security audits with the resources necessary to effectively perform the role. Approaches could include:

   — increasing the resourcing and capacity of the Australian Government’s Office of Transport Security (OTS) to enable them to conduct effective offshore security audits and inspections; or

   — transferring the security responsibility to the Border Protection Command (BPC), the Australian Maritime Safety Authority (AMSA) or another law enforcement agency with the capacity, or ability to acquire capacity, to conduct on-site compliance security inspections of offshore oil and gas facilities.

1.3 Require contract and subcontract companies to operate in accordance with the security plan of the principal operator or contractor. This will strengthen offshore security of contract and subcontract arrangements.

1.4 Amend the offshore and onshore regulatory framework by expanding the range and scope of security regulation to match that of the safety regime. This will afford protection to pipelines, offshore exploration, drilling and construction infrastructure and onshore facilities (such as processing plants and storage areas, located adjacent to security regulated port facilities) to achieve ‘whole-of-industry’ security consistency.
Active on-site exercises

2. RECOMMENDATION
The Inquiry recommends that the Australian Government and relevant state and territory governments agree to establish an active, ongoing exercise program for selected offshore oil and gas facilities, sufficient to ensure that relevant government agencies are adequately informed, practiced and prepared to mitigate or respond to a serious offshore security incident.

POSSIBLE OPTIONS
2.1 Establish a program of periodically active Australian Defence Force (ADF) and combined ADF/BPC/police exercising on, and in the vicinity of, major offshore oil and gas facilities.
2.2 Obtain agreement with industry for ADF and BPC personnel, police and other relevant agency representatives to participate in periodic familiarisation tours and deployments to selected offshore facilities—this will improve their levels of knowledge and understanding of facility infrastructure and operations and their overall level of incident preparedness.
2.3 Include sufficient government agency and private operator engagement in company and facility security planning and active on-site exercising—this will ensure that government emergency response personnel gain an accurate and realistic understanding of the knowledge, technical expertise, response and recovery skills of facility operators and other industry experts.

Access and egress security

3. RECOMMENDATION
The Inquiry recommends that agreement is reached between the Australian Government and industry on identifying consistent minimum standards of security and screening arrangements for all offshore access and service-delivery aviation and maritime ports.

POSSIBLE OPTIONS
3.1 Implement airport Regular Passenger Transport (RPT) security standards and screening arrangements, currently in place in regulated Australian airports, at onshore heliports servicing offshore oil and gas facilities.
3.2 Extend the security provisions of the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) security to cover all currently unregulated maritime ports and facilities that operate as a supply point to service offshore oil and gas facilities.
3.3 Hold consultations between the Australian Government and industry to reach agreement on the minimum security standards for access security at all heliports and maritime ports servicing offshore facilities, with such standards to be settled and observed by Memorandum Of Understanding (MOU) or regulation.
Security exclusion zones

4. **RECOMMENDATION**

The Inquiry recommends that immediate consideration is given to extending and hardening current security exclusion zone boundaries and arrangements to increase the safety and security of offshore facilities from unlawful or unauthorised intrusion and threat.

**POSSIBLE OPTIONS**

4.1 Introduce a new three-tiered approach to security zoning for all offshore facilities within Australian waters, including:

- a cautionary zone associated with traffic separation schemes, traffic lanes and recommended routes of 15 nautical miles from any offshore facility that requires vessel operators to make and maintain communication with facilities within its radius;

- an area to be avoided of 5 nautical miles from any offshore facility that acts to prohibit entry into the zone by shipping unrelated to the offshore facilities; and

- an exclusion zone, within the area to be avoided, of between 1 and 2.5 nautical miles for all shipping that is not directly related with the facility operations and to which access by can only be gained through express approval to enter given by the operator.

4.2 Establish ship routeing schemes, vessel traffic management schemes, traffic lanes and recommended routes and areas to be avoided around and in the vicinity of all offshore facilities to improve the stand-off safety distance for ship navigation around such offshore facilities.

4.3 Attribute liability for the cost of evacuation and any associated ‘shutdown’ costs to the owner or operator of a vessel who intrudes into an exclusion zone and (through the nature of the vessel’s activities) causes an evacuation of a facility—these costs to be met by the owner or operator of the intruding vessel unless the facility operator acted unreasonably in commencing the evacuation.

Government and industry interaction and relationships

5. **RECOMMENDATION**

The Inquiry recommends that active and constructive steps are taken to further improve the quality and mutual value of engagement and interaction between government and industry.

**POSSIBLE OPTIONS**

5.1 Increase industry and government engagement to improve mutual levels of understanding of the intelligence gathering, analysis and dissemination process, and the knowledge and technical expertise of industry with regard to security-related issues.

5.2 Change the current security clearance procedures to improve the access for designated industry security personnel to important threat information via a clear and transparent process that is demonstrably inclusive and equitable to industry.
5.3 Establish an MOU between the Australian Government and industry to underpin a new consultative forum, involving ADF representation, that meets regularly with industry representatives to address security-related issues and concerns, particularly in the north and north-west of Australia.

5.4 Strengthen the current whole-of-government approach to security in the north and north-west of Australia by widening the role and purpose of forums, such as the Oil and Gas Security Forum (OGSF), to include periodic engagement and interaction between the oil and gas industry, the maritime industry, the onshore mining industry and state and territory government agencies.

5.5 Review and assess the level of risk-sharing of normally restricted intelligence information with relevant industry stakeholders and weigh this against the potential consequences of not doing so.

Incident response—capacity, command and control

6. **RECOMMENDATION**

The Inquiry recommends that the Australian Government review the current reporting and command and control arrangements governing security compliance and incident response on offshore oil and gas facilities with a view to improving their clarity and effectiveness.

**POSSIBLE OPTIONS**

6.1 Review the current arrangements for command and control of federal, state and territory national counter-terrorism incidents and for reporting suspected security incidents—this will ensure the arrangements are adequately understood by all relevant parties, particularly by stakeholders of the offshore oil and gas resources sector.

6.2 Create a single ‘all-hazards’, triple zero (000) style, federal incident reporting centre for the offshore oil and gas resources sector industry.

6.3 Declare the Australian Government Crisis Coordination Centre (AGCCC) as the single, federal ‘all-hazards’ incident reporting centre for the reporting of offshore safety and security incidents, and with responsibility for:
   - the coordination of immediate response and physical assistance; and
   - the provision of advice and support to executive decision-makers within government and to industry.

Recruitment and vetting

7. **RECOMMENDATION**

The Inquiry recommends that a review is conducted of current industry recruitment and vetting processes to identify and clarify their scope, coverage, gaps and limitations and areas for improvement.
POSSIBLE OPTIONS

7.1 Initiate and maintain a briefing program to ensure that relevant industry and government representatives have an accurate and comprehensive understanding of the range and scope of Maritime Security Identification Card (MSIC) vetting and assessment and of the reality of the limitations and gaps in the current employee security vetting process.

7.2 Extend the current MSIC security vetting arrangement to cover all operations associated with offshore oil and gas exploration, construction and production activities—for example, to cover:
   - vessels under 500 gross register tonnage;
   - unregulated maritime ports;
   - supply chain operations; and
   - sub-contractor arrangements.

7.3 Initiate a consultative process between industry and government to develop and agree on mutually desired practices and standards to strengthen employee security.

Training and awareness

8. RECOMMENDATION

The Inquiry recommends that the Australian Government assist industry with identifying and implementing appropriate minimum-standard security training and awareness programs sufficient to equip facility staff with the skills and understandings necessary to competently respond to security-related threats and situations should they arise.

POSSIBLE OPTIONS

8.1 Settle mutually-agreed minimum benchmark standards for the frequency and measurement of staff security induction and refresher training on facilities, through discussions between relevant government agencies and industry stakeholders - this will ensure that relevant facility staff possess and maintain adequate levels of skill and knowledge.

8.2 Develop short awareness-training programs that are sufficient to:
   - provide selected facility workers with advice on how best to identify, report and respond to suspicious or unusual behaviour, sightings or incidents; and
   - ensure selected facility workers have a realistic, practical working knowledge of existing security plans and arrangements and their immediate-response responsibilities.

8.3 Review the current Maritime Security Guard (MSG) training framework, through joint industry and government initiatives to ensure that:
   - relevant training programs adequately meet required security standards; and
   - the training programs provide MSGs with an adequate understanding of the powers and authorities they possess under MTOFSA, and how they should be lawfully exercised.
8.4 Develop a training program for immediate-responder crime scene protection to be delivered to selected facility staff that would:

- provide guidance on how to determine, contain and protect a likely crime scene, so as to assist any criminal investigation that may follow;

- explain the importance where items or people within a crime scene are required to be moved for safety or medical reasons, of recording the original position of the item or person, and provide guidance on the evidential value of avoiding any unnecessary interference with anything within a crime scene; and

- provide guidance on the type of observations or actions that should be reported and recorded at the earliest opportunity.

8.5 Consider providing the above training courses for development under the Australian Quality Training Framework (AQTF) to serve as a national security training and assessment process to achieve industry wide accreditation consistency.

8.6 Consider the Australian National Security College as a possible training facility that industry can access on a cost-recovery basis.

Cyber Security

9. RECOMMENDATION

The Inquiry recommends that senior executive of oil and gas companies operating within the Australian environment:

- consider participating in executive cyber security training programs to ensure they have an appropriate level of understanding of the reality of the emerging cyber threat environment to business integrity and continuity;

- implement measures to ensure there is an appropriate level of understanding, at both the executive and operational levels, of the potential damage that may be caused to their business by cyber intrusion and take active steps to identify:

  - the information most critical to business continuity and integrity;
  
  - the critical risks associated with any unlawful access to information; and
  
  - the most effective way to achieve a balance between maintaining maximum levels of computer security and protection of information while facilitating the access to information necessary for efficient business operations.

10. RECOMMENDATION

The Inquiry recommends that to assist the above process the Australian Government facilitates periodic:

- Computer Emergency Response Team (CERT) presentations at OGSF, Energy Security Group (ESG) and similar forums; and

- Cyber-based exercises, targeted directly on offshore oil and gas operations with industry.
The US experience – possible approaches for Australia

11. Option to improve the knowledge and understanding of offshore facility security resilience:
   • Develop an Australian information database that will identify the capacity of selected offshore production facilities to withstand or mitigate deliberate attack.

12. Option to strengthen Australian offshore production facility preparedness:
   • Include the requirement in offshore production security preparedness plans for a pre-coordination plan that tests the capacity of an operator to respond to a ‘worse-case scenario’ incident.

13. Option for limiting the carriage of firearms and other weapons on facilities in Australia:
   • Adopt an approach that only permits firearms and other weapons to be brought onto an offshore production facility or production LNG plant in response to a specific emergency or whilst the facility or plant is operating at the highest MARSEC level.

14. Option for enhancing recovery in Australia:
   • Develop joint protocols between Australian Government, state and territory government agencies, similar to those developed between the United States Coast Guard (USCG) and US Customs and Border Protection (CBP) to facilitate the expeditious recovery of trade following an incident causing major disruption to production, supply or ports.

15. Option to test security preparedness:
   • Develop an Australian active exercising program sufficient to test the full range of government and industry responses and that includes a capacity to test the ability to respond simultaneously to multiple security incidents.

The North Sea experience – possible approaches for Australia

16. Option to improve offshore facility awareness and industry-government communication:
   • Implement an offshore safety induction and emergency training program similar to that operated by the Grampian Police which provides for deployment of relevant police to industry emergency and response control rooms and on offshore production facilities, as part of a regular familiarisation and liaison program.
The Australian experience – possible approaches

17. Options for the establishment of Vessel Traffic Service (VTS) systems to protect offshore facilities:
   • Establish a VTS system to monitor and control shipping movements along the north-west Western Australia coast in coastal and EEZ waters to enhance safety and security situational awareness.
   • Use a VTS system in conjunction with any ship routeing schemes, vessel traffic management schemes, traffic lanes, recommended routes, and areas to be avoided to ensure that ships maintain adequate safety and security distances from current and projected offshore oil and gas facilities.

18. Options to improve surveillance and situational awareness:
   • Employ close-range high-definition radar with Automatic Radar Plotting Aid (ARPA) and Automatic Identification System (AIS) capability as a standard part of offshore facility security infrastructure - this will improve the quality of offshore surveillance and situational awareness.
   • Establish an agreement between industry and government that facilitates real-time transfer of radar data to government agencies, such as BPC and AMSA. This will enhance maritime domain awareness in Australian offshore oil and gas fields.
   • Develop a link to provide data feeds to BPC, AMSA and police, where relevant.
   • Expand the current use of Closed Circuit Television (CCTV) or Infra-Red Thermal Imaging cameras to provide capacity to monitor the immediate sea area around each offshore facility.
   • Improve shore-based maritime monitoring capability using facility-based radar, AIS, CCTV and Infra-Red inputs to improve surveillance and oil-field situational awareness.
   • Use video analysis to provide an automatic surveillance capacity within the immediate sea area around a facility.

19. Options to strengthen Joint Petroleum Development Area (JPDA) and outer EEZ security arrangements:
   • Review security arrangements in the JPDA.
   • Clarify the differences between Australia’s maritime safety and security response capabilities and those of neighbouring regional countries such as Timor-Leste and Indonesia and identify the issues that may affect safety and security planning and response arrangements at the outer limits of Australia’s EEZ.

20. Option for the possible use of the Interpol Globally Verifiable Identity (GV-ID) card:
   • Companies individually, or through APPEA acting on behalf of the Australian oil and gas resources sector, enter into a partnership with Interpol, under which Interpol would verify background information on potential overseas workers, and issue an Interpol GV-ID card for such workers.
This Inquiry was conducted by the Inspector of Transport Security (the Inspector) under the authority of, and in accordance with, the Inspector of Transport Security Act 2006 (the Act). The object of the Act is to improve the security of transport and security-regulated, offshore facilities by providing for independent inquiry into security matters relevant to transport and offshore facility operations.

It is not the object of the Act to either apportion blame in relation to any matter, to provide the means to determine liability of any person, or to draw any adverse inference from the fact that a person is the subject of an inquiry into a matter. Rather, the aim of an inquiry is to provide constructive analysis and advice that may contribute to the further improvement of the security of the matter under inquiry.

Under the provisions of the Act, the Minister for Infrastructure and Transport (the Minister) may, inter alia, by direction in writing, direct the Inspector to inquire into a transport security matter or an offshore security matter that the Minister believes, on reasonable grounds, to be significant and to potentially have implications for the security of a regulated offshore facility, or of security-regulated offshore facilities in general.

Under this direction, and in accordance with the objective of allowing the conduct of an independent inquiry, the Inspector is not otherwise subject to direction from the Minister or the Secretary of the Department of Infrastructure and Transport in relation to an inquiry.

This Inquiry was formally announced by the Minister, the Honourable Anthony Albanese MP, on 1 February 2011, following an initial direction given to the Inspector by the Minister on 31 May 2010 and a formal letter of support signed on behalf of the Prime Minister on 11 November 2010.

The Inquiry terms of reference (see Appendix 1 – Terms of reference) were wide ranging and included a direction to inquire into and review:

- government and industry relationships and arrangements;
- current stakeholder and government communications and coordination capabilities;
- current security control and oversight arrangements;
- the ability of security-regulated facilities to undertake risk assessments and develop security programs;
- the extent and nature of any security gaps or weaknesses in current arrangements;
- the ability of operators to meet government security requirements;
- whether current security measures are contributing to positive security outcomes in the national interest; and
- the potential consequences—economic, environmental and human—of the violent takeover of an offshore facility.
Due to the wide nature of the terms of reference, including the number of Australian Government, state and territory government agencies potentially impacted by the inquiry, the operational phase of the inquiry was preceded by letters written to relevant ministers, to the chief executive officers of oil and gas peak bodies, and to oil and gas companies to seek their cooperation with the inquiry.

After receiving agreement from governments and industry to cooperate with the inquiry, the Inspector organised a series of introductory meetings with relevant government representatives.

The Inspector also provided a confidential briefing to the board of the Australian Petroleum Production and Exploration Association Ltd (APPEA), the peak national body for upstream oil and gas exploration and production within Australia. He asked that an industry liaison officer be nominated to work closely with the inquiry and to facilitate communication with industry and site visits to selected oil and gas facilities. Mr Bill Forbes, Vice President (then General Manager) Security and Emergency and Crisis Management, Woodside Petroleum, was confirmed as the primary contact and Mr Chris Ruff, Principle Security Advisor Corporate and People, Santos was named as an alternative.

Subsequently, the Inspector briefed industry participants at the APPEA Conference (11 April 2011) on the nature and scope of the inquiry and met with the heads of security of major oil and gas industry corporations operating in Australia.

Between April 2011 and April 2012, the Inspector and the inquiry team conducted a wide range of Australian and international consultations to review and assess security planning and preparedness, recruitment, training, government and industry interaction and engagement, command and control arrangements, response capacity and clarity, and government or industry communication and information-sharing arrangements relevant to the oil and gas resources sector environment.

To inform the Inquiry on the current international and Australian maritime law relevant to the offshore oil and gas industry, Dr Michael White Q.C., Adjunct Professor, University of Queensland, was commissioned to prepare a legal framework, research and discussion paper which was considered and referred to in the preparation of this Inquiry report.

Internationally, the Inspector looked at governance and operational arrangements in the Gulf of Mexico and the North Sea area and had meetings with government and industry representatives in the United States of America (US), the United Kingdom (UK), Norway and France, and closer to home in Indonesia and the Philippines.

Locally, consultations were conducted onshore and offshore locations in Western Australia, the Northern Territory, the Joint Petroleum Development Area (JPDA) in the Timor Sea, Queensland and Victoria. With the active cooperation and assistance of industry, offshore site assessments were conducted on facilities off the North West Shelf (NWS) and off the coast of Karratha in Western Australia, in the JPDA and in the Bass Strait, Victoria. In the US, offshore site visits were organised by the United States Coast Guard (USCG) to facilities in the Gulf of Mexico.

In addition, Australian Liquefied Natural Gas (LNG) plants, heliports, maritime supply ports, production hubs and pipelines were inspected, with comparative assessments being made of similar facilities internationally.

A total of 31 offshore and onshore site visits and more than 50 consultations were undertaken in Australia. Internationally, there were eight offshore and onshore site visits and some 45 consultations.
On 8 March 2012, an industry roundtable workshop, involving the security representatives of major oil and gas companies, was conducted in Perth, during which prima facie issues of concern, identified during the inquiry process, were tested with industry. A series of possible options for improvement were sense-checked with industry at that time.

On 29 March 2012, a similar workshop, involving representatives from the relevant Australian Government agencies, was held in Canberra and the identified issues and options were further sense-checked and tested in that forum.

The willingness of industry to openly and transparently share their safety and security practices and procedures and to facilitate and host site inspections to onshore and offshore infrastructure has been of great assistance and demonstrated the desire of industry to continue to improve their security understanding and preparedness.

Similarly, government agencies in Australia and overseas have been open and willing to share information, even when this has meant revealing perceived weaknesses or challenges in their current arrangements. Successful initiatives and innovations that have enhanced security preparedness have also been shared. The contribution these generous and frank interactions have made to the quality of this inquiry cannot be overemphasised.

In those cases where government agencies did raise different approaches to particular issues, all of the options were carefully considered in the drafting of this final report.

While a view was put during government discussions that the report should not seek to make recommendations, but rather to identify desired outcomes and the options by which these outcomes may be achieved, provisions of the Act and the importance of the issues identified during the Inquiry, combined to convince the Inspector that it was important that recommendations on the issues of primary concern be made.

A comprehensive list acknowledging those people and organisations who assisted the inquiry is included at Appendix 2: International offshore and onshore site visits and consultations and Appendix 3: Australian offshore and onshore site visits and consultations.
Introduction

The International Energy Agency key statistics for 2010 show world oil production was 3,970 million tonnes and natural gas production was 3,282 billion cubic metres. Since 1973, world oil production has increased by around 38 per cent and natural gas production has increased by 260 per cent.²

In just over 100 years the industrial world has shifted away from a reliance on coal, as the primary industrial and domestic energy source, to oil and is now looking to other sources such as natural gas and renewable energy to replace dwindling oil reserves. Energy supply is continuing to shift away from the Middle East as LNG and coal become increasingly more widely available across the globe.

Similarly, there is a global shift away from the traditional major users of energy—the US and Europe—to China, India and other Asian countries. In 2010, the International Energy Agency predicted that the energy demand of countries that are not part of the Organisation for Economic Cooperation and Development (OECD) will account for 93 per cent of the projected increase in world demand by 2035.

Currently the major global production areas include the Middle East; the North Sea; the US, including the Gulf of Mexico and Alaska; Africa; South America; South-East Asia and Australia. The most rapid rate of development is occurring in the South-East Asian region.

Australia is a major beneficiary of the global shift in energy demand and supply being rich in high quality coal and natural gas. Australia is currently the largest producer of export coal, the fifth largest producer of LNG and looks set to become the second largest producer of LNG by around 2020.

Together with other South-East Asian countries, Australia is increasingly supplying oil and LNG to a predominantly Asian market, led by China, India, South Korea and Japan. The increasing large numbers of delivery tankers traversing South-East Asian waters will create new supply-chain challenges for both importing and exporting nations including Australia.

Energy security is a major issue for bulk importers of oil and gas and—as LNG storage capacity is limited—constant, reliable delivery is vital, especially for such needs as domestic electricity generation. This is an issue of critical importance for the major importers of Australian oil and gas who rely heavily on Australian energy imports for domestic and industrial supply.

Energy supplies from the Persian Gulf have been protected for decades by the major importing nations, including the US, to ensure ongoing reliability of supply. It is not difficult to extrapolate that major importers of Australian energy may adopt a similar approach in protecting the supply route from Australia to their shores.
Australia is the world’s ninth largest energy producer, accounting for around 2.4 per cent of world energy production. Australia produces coal, uranium, LNG, crude oil, LPG and renewable energy. Oil and gas accounted for 17 per cent of Australia’s total energy production in 2008–09.

Annually, Australia’s oil and gas industries contribute 2.5 per cent of Australia’s gross domestic product and generate $28 billion in revenue. In addition, they yield almost $9 billion in direct tax payments and contribute 58 per cent of Australia’s primary energy needs.

While oil production is currently in decline in Australia, gas production is growing rapidly. LNG is widely recognised as a cleaner energy alternative to oil and coal for industrial and domestic use and worldwide demand is rapidly increasing, with production expected to rise by 50 per cent from 2011 levels to meet demand.

Current LNG projects, and those under development or consideration, exceed $200 billion in investment and, with long-term contracts and projected 25-year production fields, will contribute significantly to Australia’s future economic wellbeing.

Consequently, the security and reliability of oil and gas production is becoming increasingly important. Of particular concern, are those oil and gas facilities operating offshore within Australia’s Exclusive Economic Zone (EEZ).

Although the total number of facilities currently operating in Australian waters is low, compared to those operating in the Gulf of Mexico or the North Sea, many of those in Australian waters are large, situated a significant distance off shore and in remote locations.

Some 3,900 facilities are in operation within the US Outer Continental Shelf (OCS), but only about 57 are currently subject to security audits and regulation. Within the Australian EEZ all offshore production facilities are required to have security plans and are liable to regulation. The number of Australian production facilities is subject to change, but is currently about 70.

Against this background, and consistent with the provisions of the Inspector of Transport Security Act 2006 (the Act), the current inquiry has focused primarily on assessing the state of affairs or matters that may reasonably be believed to have significant implications for security-regulated offshore facilities in general.

In comparative terms, Australian industry practices and its government or industry relationships and arrangements generally reflect those practices and arrangements in place in other countries.

However, as identified in earlier inquiries, there are counter measures to every initiative and terrorist style attacks continue to demonstrate that terrorist and criminal groups and determined lone perpetrators are adaptable, unpredictable and adept at developing new methods to breach security or commit crimes.

Although Australia can be confident that the security measures and practices in place generally reflect those in effect elsewhere, areas of vulnerability in current security-related practices and arrangements that warrant consideration and improvement have been identified through this Inquiry.

In considering these matters, however, it is important to recognise that other countries visited during the inquiry are dealing with similar challenges and that, internationally, an ongoing evaluation of the security effectiveness of oil and gas infrastructure is occurring with the aim of continuing to improve the quality of security-related outcomes.
Recent measures and initiatives introduced in the US, the UK and Norway may provide useful guidance to any review of the security of the Australian oil and gas resources sector and are considered in this report.

In accordance with the Inquiry terms of reference, this report attempts to assess the quality and effectiveness of current security arrangements and response capabilities of both oil and gas operators and government. In this assessment particular emphasis is given to:

- the whole-of-government approach to offshore oil and gas infrastructure security, including, where relevant, areas for improvement;
- the quality of current industry security arrangements and practices, including the extent, type and effectiveness of security training, assessments, drills and exercise regimes within the offshore oil and gas environment;
- the clarity and effectiveness of government lead-agency command and control, and response arrangements and capabilities; and
- the resources that government or industry are likely to require to respond to a security incident involving offshore oil and gas infrastructure.

As part of this evaluation, this report contains an outline of the nature and size of the global and Australian oil and gas industry; a summary of the international meetings and site visits conducted during the inquiry; an explanation of the lessons learnt and practices identified in the countries visited, and an examination of the security arrangements currently in place within Australia’s EEZ.

The recommendations and options listed in the report arise from this evaluation.

Recommendations have been made where it is considered the issue identified is sufficiently significant to warrant early consideration of change and action.

Where options form part of a parent recommendation they are intended to simply suggest ways by which the recommendation could be addressed. These include courses of action that reflect initiatives that have been successfully implemented in other parts of the world.

Where options are listed without a parent recommendation, the intention is to cause consideration of the relevant subject matter and the existing arrangements, and to offer a way by which change, if considered necessary, could be achieved.

In assessing the matters of concern identified in this Inquiry, this report does not attempt to provide a prescriptive report card on the state of security effectiveness and preparedness in the oil and gas resources sector environment. Rather, the report attempts to provide impartial and, hopefully, constructive advice to industry and government stakeholders that may be of value in the further and ongoing review and improvement of offshore oil and gas industry security measures.

There is a degree of deliberate repetition within the body of the report due to the importance of dealing with issues holistically and presenting, wherever possible, a cohesive and inclusive outline of matters under review.
International maritime law

The global oil and gas sector is composed of multinational companies who engage in exploration, drilling and production and a diverse range of specialist operators who undertake functions such as drilling, capping, servicing, transporting, and provide heliports and pipelines. These global operations are subject to international law as well as the law of the country in whose waters the operations are taking place.

The United Nations Convention on the Law of the Sea (UNCLOS) defines the rights and responsibilities of nations in their use of the world’s oceans, establishing guidelines for businesses, protecting the environment, and managing marine natural resources.

Five offshore zones are defined by the UNCLOS and extend from a baseline, which is normally the low-water line along the coast of a country.

- The first zone is the territorial sea and extends up to 12 nautical miles from its baseline. Except for innocent passage and other rules of international law, a state has sovereignty over this area.
- The contiguous zone is the second zone and extends from 12 nautical miles from the outer edge of the territorial sea up to 24 nautical miles from the baseline. In the contiguous zone, a state may enforce customs, fiscal, immigration or sanitary laws and regulations.
- The third zone is an EEZ and extends to a maximum of 200 nautical miles from the baseline, unless it is curtailed by a maritime boundary with another state. A coastal state has exclusive jurisdiction over all natural resources, living and non-living, within its EEZ, including fishing, mining and oil and gas exploration and exploitation.
- The continental shelf is a legal and a geographical phrase and constitutes the fourth zone. In its legal use, as set out under UNCLOS, a coastal nation may claim rights over the OCS beyond its EEZ according to a complex formula set out in UNCLOS. The result is that if the continental shelf is continuous offshore, then the coastal state may lodge a claim, with the relevant commission under UNCLOS, over up to a maximum of 350 nautical miles from the baseline or 100 nautical miles from the 2,500 metre depth contour line. Australia has done this and the commission has approved nearly the entire claim. A coastal nation has control of all natural resources in the seabed or subsoil in its OCS (but not in the water column).
- The final and fifth zone, the high seas, includes those areas beyond the jurisdiction of any state, which usually means beyond the EEZ. On the high seas states have very limited powers except in relation to their own ships, aircraft or citizens.

The UNCLOS determines the laws a coastal state may pass and enforce for a zone, but other conventions and codes also apply.
Around Australia there is, in addition to the various UNCLOS maritime zones, a framework of national maritime zones that rules Australia’s 12 nautical miles territorial sea. This framework is the result of an agreed division of responsibilities between the federal, state and territory governments, and falls under Australian legislation. For an area that extends three nautical miles seaward from the territorial sea baseline—determined by the Coastal Waters Limit—the title to the seabed and the rights to the water column lie with the Australian states and the Northern Territory. Through the Offshore Constitutional Settlement in 1983, the adjacent state or territory’s legislation applies to this area. The states and Northern Territory were also accorded legislative powers over that area. Beyond that three nautical mile area, the responsibility remains with the Australian Government.4

After the terrorist attacks of 11 September 2001, the IMO developed the International Ship and Port Facility Security Code (ISPS Code). The ISPS Code covers security measures for ships and port facilities and has been included as an amendment in the Safety of Life at Sea Convention, 1974 (SOLAS Convention) to which Australia is a party.

The objectives of the ISPS Code are to:

- establish an international framework for cooperation between contracting governments, government agencies, local administrations and the shipping and port industries to detect/assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;
- establish the respective roles and responsibilities of all the parties concerned, at the national and international level, for ensuring maritime security;
- ensure the early and efficient collation and exchange of security-related information;
- provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
- ensure confidence that adequate and proportionate maritime security measures are in place.

The objectives are addressed in the security plans for each ship and port facility and appropriate security officers and personnel on each ship, in each port facility and in each shipping company implement the objectives. There is enough flexibility in the code to tailor the security measures to the specific risks faced by each ship or port facility. The code has two parts, a mandatory part that covers the appointment of security officers for shipping companies, individual ships and port facilities, and a guidance and recommendations part that covers the preparation of security plans for ship and port facilities.5

**Australian maritime law**

For Australia, the UNCLOS Convention created a vast maritime domain out to the limit of the EEZ, with an extended continental shelf substantially larger than the Australian continent in area.

As well as defining ocean boundaries, the UNCLOS Convention establishes general obligations for safeguarding the marine environment and creates a legal regime for controlling mineral resource exploitation in deep seabed areas beyond national jurisdiction.
In Australia, a state or territory’s coastal waters are defined by the Coastal Waters (State Powers) Act 1980 and the Coastal Waters (Northern Territory Powers) Act 1980 as extending three nautical miles from its baseline. The state or territory may make laws applying to the coastal waters and the seabed, subsoil beneath and the airspace above. The Commonwealth still exercises responsibility over a state or territory’s coastal waters in relation defence and foreign affairs.

The Commonwealth Acts Interpretation Act 1901 also has application and states that, unless otherwise provided, each Act is to apply in the coastal sea as if it were part of Australia and any reference to Australia or to the Commonwealth is to be read as including the Australian coastal sea.

In summary, states and territories have jurisdiction out to the limit of three nautical miles from the baselines if they choose to exercise it. From there to the outer limits of the OCS (the ‘offshore area’) the Commonwealth has jurisdiction, but there are many exceptions. Two of them are that some Commonwealth laws apply to the coastal state law in the offshore area. These are known as applied provisions, and the states are invited to seek approval to have the Commonwealth laws applied.  

Ultimate responsibility for Australia’s offshore areas, beyond three nautical miles from the territorial sea baseline, rests with the Australian Government, whereas in ‘coastal waters’, onshore and as far as three nautical miles seaward of the baseline, petroleum operations are the responsibility of the individual state and territory governments.

**Maritime Transport and Offshore Facilities Security Act 2003**

The Australian Government developed the *Maritime Transport Security Act 2003* (MTSA) to implement the ISPS Code in Australia. Both the ISPS Code and MTSA came into effect on 1 July 2004.
In 2005, MTSA was extended and renamed the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA). The amended Act, and regulations under it, establishes the legislative basis for approving security plans for offshore oil and gas facilities.

The safety and security zones around offshore facilities are defined by the UNCLOS Convention and *IMO Guidelines on safety zones and safety of navigation around offshore installations*. These zones can extend up to 500 metres out from a fixed or floating offshore facility and its associated wellheads and pipelines.

In Australian waters, MTOFSA defines the security zones around offshore oil and gas production facilities in Australia’s EEZ and territorial waters, but does not cover offshore oil and gas exploration, construction or pre-production activities.

The Australian Government’s Office of Transport Security (OTS) in the Department of Infrastructure and Transport administers the MTOFSA and Regulations.

The purpose of the MTOFSA is to safeguard against terrorism and unlawful interference with maritime transport or offshore facilities. Under the MTOFSA, regulated offshore facilities are required to comply with offshore security plans, approved by the Secretary of the Department of Infrastructure and Transport, and have a number of other legal obligations relating to compliance and reporting.

Security regulation focuses on those assets thought to be at greatest threat or risk, and does not comprehensively cover all assets in the industry. For example, offshore facilities involved in the production process must have an offshore security plan, but not offshore facilities engaged in the exploration, construction or pre-production phases of operation. Floating Product, Storage and Offtake units (FPSO) and Floating Storage Unit (FSU) ships, which can act as offshore facilities, are regulated.

One of the major provisions in the legislation was the introduction of a new security identification card for maritime workers. The MSIC is a nationally consistent identification card issued to a person who has been the subject of a background check. It shows that the holder has met the minimum security requirements to work unescorted or unmonitored in a maritime security zone. Applicants must undergo a background check that is coordinated by AusCheck, a division of the Attorney-General’s Department, before an MSIC can be issued.

The *Defence Act 1903* under Part III AAA creates powers for the ADF to act with lethal force with regard to the protection of designated critical infrastructure. Part III AAA, however, can only be enacted jointly by the Defence Minister and the Attorney General if it can be clearly demonstrated to their satisfaction that a situation exists within which there is the potential for loss of life.

In the offshore oil and gas environment, in the event that a rig or facility had been fully evacuated and the threat posed was only of economic or environmental impact, it would be unlikely that Part III AAA could be activated and the response would be a matter for local police or other authorities. Involvement of defence resources in these circumstances would be the subject of negotiation, but the ADF will not usually become involved unless there is a threat to life.
The vast majority of facilities or infrastructure likely to be considered for designation as critical infrastructure are situated within Australia’s self-governing states or territories. As a consequence, most of the critical infrastructure lists are initially determined by the relevant state or territory and then supplied to ASIO and the National Counter Terrorism Committee (NCTC) for assessment. This process is assisted by a risk framework, developed by ASIO, and provided to the states and territories to help them identify the likelihood and consequence criteria that can be used to determine the Critical Infrastructure (CI).

Infrastructure determined to be appropriate for designation as CI under Part III AAA of the Defence Act 1903, which includes offshore areas, will be declared in writing as designated CI under Section 51CB by one or more of the relevant ministers (the Prime Minister, Minister for Defence or the Attorney-General).

As a consequence of this process a large number of facilities have been listed by the states and territories as CI although only about 30 have been identified by the Australian Government as nationally vital CI.

Within the private industry environment, private owners and operators can identify their infrastructure as critical and can then negotiate with relevant state or territory police to establish whether the infrastructure should be placed on the state or territory CI list. Once declared as CI the relevant state or territory police then work with the owners or operators to gain an understanding of the operation of the facility and how best to respond to an incident should it occur.

With the exception of Victoria, there are currently no legislative responsibilities placed on owners, operators or relevant government agencies as a consequence of the designation by state or territory of a piece of infrastructure as CI.

Within Victoria, CI is governed by the Community Protection (Terrorism) Act 2003 under which owners and operators are required to exercise with police and to implement risk assessments and plans for each designated facility.

With regard to the oil and gas industry however, the only facility within Victoria currently designated as CI under their Community Protection (Terrorism) Act 2003 is the Longford Gas Plant, which is based on the mainland.

Currently no offshore Victorian facilities have been designated as CI and as a consequence they are governed by the same security arrangements as apply to the rest of Australia.

In the operational sense, the Attorney-General’s Department is of the view that the ESG and OGSF are the best forums to consider and deal with CI classification which have been broadened beyond terrorism to embrace an all hazards approach. With the exception of Victoria however, which requires mandatory risk assessments, there is no mandatory requirement for owners or operators of CI to conduct risk assessments in any of the other states or territories, although government advice may suggest it is appropriate for them to do so. Under current Australian Government arrangements, the emphasis is that private industry has responsibility for ensuring the safety of their infrastructure and assets.
The inquiry team visited government and industry organisations overseeing or operating facilities in the Gulf of Mexico, the North Sea, Indonesia and the Philippines to look at the way other countries are monitoring and regulating their oil and gas resource sector security arrangements and dealing with the particular security challenges of their region.

The purpose of the meetings and site visits was not to assess and report on the security performance of other countries, but rather to explore the various regulatory frameworks and security practices used and to learn from the experience of countries that may have more fully developed and tested security arrangements.

A brief summation of the role of the various organisations consulted and the site visits made is given below under the country headings, followed by a review of the policy and practices most relevant to the Australian oil and gas industry. Appendix 2: International Offshore and Onshore Site Visits and Consultations contains a complete list of the inquiry team’s consultations.

**United States—Gulf of Mexico—oil and gas operations**

The Gulf of Mexico is the major oil and gas producing region of the US and accounts for about 29 per cent of US crude oil production and 12 per cent of natural gas. Currently about 3,132 of the total of 3,900 oil and gas facilities on the US OCS are active production facilities. Over 40 per cent of US petroleum-refining capacity is located along the Gulf of Mexico coast, as well as almost 30 per cent of natural gas processing plant capacity.4
In the US, there are currently some 240 government standards directly applicable to oil and gas production. Strong government-to-government relationships exist within the US environment, with clear understanding across agencies of other agency responsibilities as well as their own remit.

**Agencies visited by the inquiry team**

The inquiry team’s site visits and meetings were conducted in Washington, Boston, Houston and New Orleans. They met with the United States Coast Guard (USCG), the Government Accountability Office (GAO), the American Petroleum Institute (API), Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), ConocoPhillips, ExxonMobil, Chevron, Eni Petroleum, BHP Billiton, Apache, Shell, BP and the Louisiana Offshore Oil Port (LOOP).

**United States Coast Guard**

The USCG is one of the five armed forces of the US and the only military organisation within the Department of Homeland Security. It has primary responsibility for the security of oil and gas operations and, until recently, shared some responsibilities with the BOEMRE. However, on 1 October 2011 the Bureau of Ocean Energy Management (BOEM) and the Bureau of Safety and Environmental Enforcement (BSEE) replaced BOEMRE as part of a major reorganisation of offshore oil and gas management.

The work of the USCG is carried out under federal regulations, specifically the United States Code: Title 33—Navigation and Navigable Waters, which covers all maritime land based security arrangements and offshore security arrangements in the US.
Operations in the Gulf of Mexico are the responsibility of the USCG Eighth District, headquartered in New Orleans. They protect 1,200 miles of coastline and 10,300 miles of inland navigable waters. The Eighth District is home to two of the nation’s busiest ports, New Orleans and Houston and seventeen of the top forty busiest ports by tonnage.

The USCG have primary responsibility for the security audit regime across the oil and gas industry and conduct regular audits on floating facilities, including annual reviews that encompass 20–40 per cent of a facility’s operations with a larger, full examination conducted on the entire facility every three to five years.

The USCG carries out about 57 audits each year, checking a range of security and safety related policies, procedures and equipment. The implementation and maintenance of set standards, exercise drills, training and employee knowledge of security or safety plans may all be the subject of review.

Prior to a planned audit, the owner or operator of the offshore facility is usually advised of the inspection, which will generally occur 90 days before or after the expiry of the current certificate under the United States Code of Federal Regulations 33. Notification ensures minimal disruption to the facility’s work schedules and business operations, and enables attendance of key personnel, such as the facility manager, at times suitable to the USCG. It is the responsibility of the owner or operator of the facility to ensure an inspection is carried out prior to the expiration of the current certificate.

**Area Maritime Security Committee**

The Area Maritime Security Committee (AMSC) is an important consultative interface between the USCG and industry. The AMSC brings together representatives from various organisations in a port to assess security risks to the port and to determine appropriate risk-mitigation strategies. Apart from port, facility, vessel owners and operators and port labour organisations, AMSC membership usually includes USCG and federal, state and local law-enforcement and emergency-response personnel.

**Bureau of Ocean Energy Management**

The Bureau of Ocean Energy Management (BOEM) has responsibility for managing environmentally and economically responsible development of the nation’s offshore resources. Its functions include offshore leasing, resource evaluation, review and administration of oil and gas exploration and development plans, renewable energy development and environmental reviews, including National Environmental Policy Act analyses and compliance documents for each major stage of energy development planning.

**Bureau of Safety and Environmental Enforcement**

The Bureau of Safety and Environmental Enforcement (BSEE) is responsible for safety and environmental oversight of offshore oil and gas operations, including issuing permits, and inspecting offshore oil and gas operations. BSEE functions include the development and enforcement of safety and environmental regulations, permitting offshore exploration, development and production, inspections, offshore regulatory programs, oil spill response and newly formed training and environmental compliance programs.

The OCS Lands Act authorises and requires the BSEE to provide for both an annual scheduled inspection and a periodic unscheduled (unannounced) inspection of all oil and gas operations on the US OCS. The annual inspection examines all safety equipment designed to prevent blowouts, fires, spills, or other major accidents.
The BSEE inspectors perform these inspections using a national checklist, called the Potential Incident of Noncompliance list. This list is a compilation of compliance elements derived from all regulated safety and environmental requirements.

**Government Accountability Office**

The Government Accountability Office (GAO) is the agency with primary responsibility for overseeing the performance of federal government agencies. The GAO is an independent agency with responsibility to examine the performance and accountability of federal government agencies and to provide objective and reliable information and analysis to Congress. As part of this process the GAO conducts periodic audits of federal government agencies such as the USCG and analyses and reports to Congress on their policy performance and the effectiveness of their programs.

**Overseas Security Advisory Council**

Government and industry liaison and interaction is assisted by the Overseas Security Advisory Council (OSAC), which is comprised of private industry, interest groups and government agencies. OSAC is part of the US Department of State, Bureau of Diplomatic Security. The OSAC was created in 1985 to promote security cooperation between American private sector interests worldwide and the US Department of State and enjoys a reputation for effectiveness and credibility.

The OSAC website [www.osac.gov](http://www.osac.gov) provides daily security updates and a range of reports on security issues such as cyber security, regional security, crime and safety, travel warnings and has an extensive resource library. OSAC subscribers have access to more detailed information and reports.

**American Petroleum Institute**

The American Petroleum Institute (API) is the leading oil and gas industry body in the US and is open to all industry operators and contractors. It currently has approximately 470 members, representing about 50 oil and gas companies.

The API has established more than 500 industry standards aimed at developing strong and robust practices that cover all aspects of exploration and production, including safety, environmental and security issues.

**Louisiana Offshore Oil Port**

A facility of particular interest visited during the Inquiry is the Louisiana Offshore Oil Port (LOOP). The LOOP is a privately owned, deepwater port off the coast of Louisiana near the town of Port Fourchon. It is regulated under a combined onshore and offshore USCG security plan.

The LOOP provides offloading and onshore oil storage services for crude oil transported on Very Large Crude Carriers (VLCCs), most of which are too large for coastal and inland ports. It currently handles 13 per cent of the US oil imports, about 1.2 million barrels a day, and connects by pipeline to 50 per cent of the US refining capability.
The LOOP has a range of maritime security measures in place, including a dedicated security patrol boat in continuous operation within the LOOP restricted zone. The patrol boat escorts ships to and from unloading buoys and the entry channel, and conducts random patrols around the whole LOOP restricted zone. The boat carries a long-range acoustic device for warning small craft and commercial fishing vessels when they are approaching or are within the restricted zone. The pre-recorded messages (in English and other languages) and siren can be heard and clearly understood up to a distance of approximately 200 metres.

The LOOP also has CCTV coverage of the approach channel and a restricted area around the VLCC oil discharge buoys. All personnel must have Transport Worker Identification Credential (TWIC) identity cards to work at the LOOP offshore and onshore facilities. A control centre at Galliano (a centre some 70 kilometres from the offshore terminal facility) monitors all oil discharge, storage, and pipeline transfer operations, and includes a separate security control room to monitor security at all the LOOP facilities.

There is strong engagement with federal agencies and good communication flow between the LOOP facilities and state security and policing authorities. There are also regular exercises and practice drills on onshore and offshore LOOP facilities. Some are conducted as joint exercises and can involve the USCG, the Federal Bureau of Investigation (FBI), the US Navy SEALS and local sheriff special weapons and tactics teams.

Whilst there are currently no LOOP style operations in Australian waters, there are sufficient similarities between LOOP operations and pending production facilities in Australia, such as on Curtis Island within the Port of Gladstone, Queensland, Barrow Island in Western Australia, and the new Prelude Floating LNG (FLNG) processing, storage and offload vessel planned for location in the Timor Sea.

As in the Australian environment, heliport access and egress security is identified within the US as an issue of key security concern. The PHI Boothville Heliport in Louisiana, which operates a contract with Shell to transfer people and stores to offshore facilities, was identified as an example of leading-edge practice. Within the contract arrangements, Shell employs full aviation-style security screening arrangements for all personnel, baggage and stores travelling by helicopter to Shell offshore facilities. Through these and similar arrangements, Shell meets the Transport Security Administration, USCG and Federal Aviation Administration security requirements for all offshore helicopter flights.

To meet these security requirements, a separate secure area that includes check-in desks, security screening, a segregated flight waiting area, briefing rooms for helicopter safety induction and an external secure baggage and stores area must be provided by the operator. Other companies operating within US OCS waters have similar security arrangements.

**Inquiry observations and options for Australia**

The Deepwater Horizon explosion in April 2010 demonstrated the significant and far reaching consequences of underestimating the secondary economic impacts of an incident on OCS facilities or deepwater ports, whether accidentally or deliberately caused.

Even in the heavily populated Gulf of Mexico region, the incident response encountered numerous challenges. By the time the well was sealed, nearly three months later, over four million barrels of oil had spilled into the gulf. Additionally, the spill caused significant environmental damage and impacted severely on workers, particularly professional fishermen, and businesses more generally. A conservative estimate of compensation costs relating to this damage is in the billions of dollars.
**Methods to assess risks**

Currently, about 28 per cent of US oil and gas production comes from about 3,900 offshore platforms. However, platforms are increasing in size as production fields move into deeper waters. The larger platforms can have up to 100 to 150 personnel.\(^{11}\)

These new large-production-capacity facilities that are being increasingly used in deepwater at the outer extremes of the US EEZ are similar to current and projected Australian offshore facilities in size, capacity and remoteness.

Within the US jurisdiction the USCG and the FBI share responsibility for preventing and responding to terrorist or criminal incidents in the maritime environment, including incidents involving energy tankers. Steps are underway for the USCG and FBI to develop an operational plan to integrate the national oil spill and terrorism response plans.

A recent GAO report\(^ {12} \) identified that energy tankers continue to face risks from terrorist groups, as demonstrated by the incident involving the MV Star in the Strait of Hormuz in 2011, which was a suspected terrorist attack.

Risks from terrorist groups to offshore energy infrastructure, such as deepwater oil rigs, include ramming by a small boat with explosives, attacking underwater by divers with explosives, a collision by an aircraft, or sabotage by an employee. The USCG evaluates the security of such infrastructure through a risk-assessment model that calculates the threat, vulnerability and consequences of an attack. In the context of this Inquiry, it is noted in the GAO report that the risk-assessment process is hindered by the limited nature of current data on vulnerabilities and consequences.

Also, Mobile Offshore Drilling Units (MODUs) such as the Deepwater Horizon, are considered vessels and not facilities, so they fall outside the USCG’s current offshore security regulations, and no security assessment is done. The Deepwater Horizon explosion, while an accident, demonstrated the potential consequences of an explosion on a MODU.\(^ {12} \)

In some areas, specific security actions have been taken as part of a public-private partnership aimed at improving the security and safety of facilities, employees and any surrounding communities. As an example, in the Houston Ship Channel night-vision and motion-activated technology has been installed and patrols are conducted on land and on the water.

To assist in prioritising its security regulatory responsibilities the USCG has developed a Maritime Security Risk Analysis Model (MSRAM). MSRAM provides an empirical basis upon which to assess security risks to offshore energy infrastructure and the challenges that may be faced in making such assessments.

Consideration is being given to developing explicit performance measures for emergency response capabilities and using them in risk-based analyses to identify and set priorities for acquiring required response resources. The USCG has identified that it may not have sufficient data on the ability of an OCS facility to withstand a deliberate attack and is taking steps to increase its database information to remedy this potential deficiency.

The USCG uses MSRAM to examine the security risks in offshore OCS facilities and to deepwater ports. This assessment is made by assessing three main factors: threats, vulnerabilities and consequences.
Under the MSRAM umbrella, various attack scenarios are assessed. Such scenarios may include an attack by a hijacked vessel, insider sabotage, or attack by a diver. Analysts then use MSRAM to evaluate vulnerabilities of individual OCS facilities or deepwater ports by assessing issues such as the capacity of an operator or other key stakeholder (including a government agency) to interdict an attack or the ability of a targeted facility to withstand an attack, and then determining the probability that an attack would be successful.

Based on the assessments of these consequences and evaluations of threat and vulnerability, MSRAM produces a risk index number for each OCS facility and deepwater port. Additional threat scenarios are added periodically to the MSRAM data set.

11. Option to improve the knowledge and understanding of offshore facility security resilience:
   - Develop an Australian information database that will identify the capacity of selected offshore production facilities to withstand or mitigate deliberate attack.

Audits and inspections

On-site offshore facility audits and inspections are regularly conducted within the US environment by the USCG and BSCE.

Annual examinations are conducted on drilling rigs or units and on crewed and remotely operated facilities. The drilling unit inspections include onboard audits, comprising two separate inspections, one of the marine section and one of the drilling section.

USCG site audits and inspections cover the implementation and maintenance of safety and security standards, exercise drills, training standards and programs, security, and testing of employee knowledge of both safety and security plans. The central aim of this inspection process is to ensure that operators are ‘playing by the rules’.

The practical difficulties associated with offshore facility audits and inspections are, however, recognised and need to be understood. Weather conditions, fuel issues, helicopter and helipad requirements and demands, helicopter escape training and competing resource demands all impact on audit capacity.

Industry’s approach to security appears, understandably, to be heavily focused on prevention rather than response capabilities. While industry security or safety plans require a pre-coordination plan that identifies a ‘worse-case-scenario critical incident’ situation and details how an operator, or company, would respond, there is a joint recognition that industry response capacity to an intentional security incident may be limited and that government has a share of the responsibility. Importantly, the pre-coordination plans are exercised annually.

All USCG inspections are conducted by either sworn or unsworn USCG members. No contractors are engaged for audit and inspection work. While safety is recognised as a higher concern in the offshore environment than security, security preparedness assessment is included in the inspection process.

The USCG are responsible for transfer arrangements and have contracts in place with helicopter companies to provide transport to and from offshore facilities. The owner or operator of a facility is responsible for meals and accommodation for the USCG inspection team. However, the inspection team must be prepared to stay offshore overnight or leave early and return later if changing weather conditions prohibit helicopter flights. The offshore weather conditions are assessed each day to see whether they are suitable for helicopter transfers.
The audit and inspection program includes well control, sub-sea controls and response (safety mechanisms and devices), regulatory compliance, drilling and production. As a basic test of security preparedness USCG will require an operator to upgrade the Maritime Security (MARSEC) level and will then test the response capacity against the increased security requirements.

However, all inspections, while firm and often conducted with no or minimal advance notice, are conducted in a constructive and partnership manner with regulatory sanctions kept as an instrument of last resort.

12. Option to strengthen Australian offshore production facility preparedness:
   - Include the requirement in offshore production security preparedness plans for a pre-coordination plan that tests the capacity of an operator to respond to a ‘worse-case scenario’ incident.

The offshore inspection process varies according to the rig or platform being inspected and the current work requirements of the operation. Not all systems and equipment need to be checked on every inspection visit. The USCG endeavours to cooperate with the operators of the offshore facility to minimise work disruptions.

A typical inspection format could include:

- a meeting with senior staff on the facility;
- the provision of general information on the inspection process and agreement on the inspection schedule;
- determination of the safety and security drills to be executed and observed;
- a documents check for current validity;
- a physical examination of the hull, equipment and fittings;
- machinery examination and testing;
- the checking of bridge and radio equipment; and
- the checking of environmental control systems for any over-the-side discharge of materials and liquids such as drill mud, chemicals and waste water.

As witnessed during inquiry team visits to offshore facilities to observe USCG audits, the inspection process incorporates security focused assessments into all relevant aspects of their inspections.

Importantly the USCG is itself subject to periodic audit from the GAO.

The security issues that US-based companies identified as ‘areas for improvement’ included:

- lack of feedback and follow up to incidents by local enforcement agencies;
- the need to create a firm security perimeter as currently only a 500 metres safety zone is enforced;
- improved control over ship movements within oil and gas fields;
- improved aerial and small-target radar coverage;
- more in-depth follow-up from government agencies when incidents, including vessel intrusions, are reported; and
- the current extent of TWIC identity card coverage and integrity as an identification authority.
These issues are very similar to those identified by industry within the Australian context.

**Carriage of firearms and other weapons**

An issue of concern in the US that has been identified as a problem within Australia relates to the carriage of firearms and other weapons by law enforcement officers on hydro-carbon rich facilities. Under US legislation the definition of a dangerous device does not unambiguously include a firearm, although one approach adopted is that weapons are only permitted onboard a production facility at the highest MARSEC level.

An agreement to adopt this, or a similar, approach within the Australian environment would remove the current uncertainty and unpredictability surrounding the carriage of weapons, by law enforcement officers on facilities within Australian waters and land based oil and gas production facilities.

13. **Option for limiting the carriage of firearms and other weapons on facilities in Australia:**

- Adopt an approach that only permits firearms and other weapons to be brought onto an offshore production facility or production LNG plant in response to a specific emergency or whilst the facility or plant is operating at the highest MARSEC level.

Within the US jurisdiction, some companies have a ‘no weapons on facilities’ policy that may override regulatory controls and apply regardless of the regulations in place.

**Incident response and recovery enhancement**

In terms of resilience, the US has a range of mitigation and recovery strategies. The GAO reported that the economic consequences of a terrorist attack on a tanker could be significant, particularly where it caused the closure of one or more ports. Some ports are therefore incorporating economic recovery considerations into their port security plans.

The USCG and the US Customs and Border Protection (CBP) have developed joint protocols for the Expeditious Recovery of Trade. These protocols establish a clear communications process and identify how the USCG and CBP will coordinate with each other, other federal agencies and the maritime industry to facilitate recovery and the resumption of trade following an incident that causes major disruption to the ports or supply systems.

The principles that are vital for an integrated response to an incident have been identified by the GAO as:

- protecting public safety and the environment;
- conducting an investigation; and
- restoring shipping (production) operations in a timely manner.

The GAO also considers that, for an integrated response, the operational response plans need to be ‘explicitly linked’ and the roles and responsibilities of all stakeholders clearly defined.12
14. Option for enhancing recovery in Australia:

- Develop joint protocols between Australian Government, state and territory government agencies, similar to those developed between the United States Coast Guard (USCG) and US Customs and Border Protection (CBP) to facilitate the expeditious recovery of trade following an incident causing major disruption to production, supply or ports.

As part of the response framework within the US, 10 major companies have established the Marine Well Containment Company (MWCC). Each company has an agreement to respond jointly in aid of a member company that suffers an incident or spill.

In the event of an incident, the MWCC will coordinate equipment mobilisation and participate on the response team under the direction of the responsible party. The MWCC will supply initial stock of dispersant fluid to the responsible party for subsea injection. The company responsible for the incident is also responsible for removing debris, relief well drilling and deploying and operating the equipment.

As follow-up to any incident, MWCC captures lessons learned and provides support for refurbishment and return of MWCC equipment. The responsible party for an incident would be responsible for refurbishing and returning the equipment.

The MWCC operates in a similar manner to the Australian Marine Oil Spill Centre (AMOSC) oil spill response company.

Twenty-four smaller companies in the US have established a similar oil spill response company structure.

It is understood the GAO is reviewing how these arrangements will work in practice and is checking the actual response capacity of the companies concerned, including assessing how they may handle two simultaneous incidents.

Additionally, oil spill response mechanisms operate in each major supply port and, while privately run and unregulated, they have some capacity to respond to an incident and act as a private industry first-response mechanism.

The security threshold for regulatory oversight is governed by the United States Maritime Transportation and Security Act and is set according to production or personnel thresholds. If a facility produces more than 100,000 barrels of oil per day, or 200 million cubic feet of natural gas per day, or hosts more than 150 persons on the facility for 12 hours or more in each 24-hour period continuously over 30 days or more it will be subject to security regulation.

There are some concerns over these thresholds, however, and it is understood they are being reviewed to lower the thresholds and increase the number of facilities subject to security regulatory oversight.

New regulations are intended to further identify ‘all-hazards’ protections and requirements, with modelling and risk assessments conducted and exercised against an ‘all-hazards’ framework to establish appropriate risk-mitigation strategies.
Standards and guidelines for industry

Within the US, the API plays a significant role in developing robust guidelines and standards of industry practice, providing some confidence to government in the ability of industry to responsibly self-regulate.

The US federal government has referenced a number of API standards that have been accredited as ‘consensus standards’. This process has contributed to the continuing development of a constructive relationship between government and industry that is predicated upon mutual benefits. Whilst additional terms and requirements may be made by government agencies to an API standard, the move to reference standards as accredited is recognised as potentially more effective than an arbitrary regulatory approach.

Of particular interest is that API has developed a security vulnerability assessment that, it is intended, will become a recommended practice or standard in the industry. A standard sets the criteria and explains how to conduct the assessment, details competency requirements and allows for technological advances.

Although the development of a standard usually takes about three years, standards can be developed much more quickly, as was evidenced after the Deepwater Horizon incident when standards were developed and implemented within six months.

An annual standards plan, published in a Federal register is available on the API website <www.api.org> with some 220 standards having global relevance.

The then BOEMRE saw referencing a standard developed by API as more effective than an arbitrary regulatory approach, even though BOEMRE may add terms and requirements to an API standard.

Despite these arrangements, however, there has been a move towards increased external third-party audits to address concerns that API and government regulators may, at the time of Deepwater Horizon, have been too close. In such audits, the third-party certifies and accredits the safety and security standards.

Consistent with a safety case approach, US regulators are looking more closely at licensing or permit risk factors and assessing what information is needed to ensure effective operational quality assurance. Questions include:

- Are emerging risks being identified?
- Are inspections focusing on the new issues?
- Are regulators and industry talking to each other so that all parties are aware of changes to plans that may occur during development?

In security-risk assessment terms there is a clear understanding in the US that onshore hubs are at the highest risks of deliberate attack. Rigs and facilities are recognised as difficult to damage as they are designed to shut down, whereas the onshore hub, where pipes, production facilities and pipelines meet, are largely unprotected and considered difficult to secure.

The new US regulatory framework aims to regulate maximum impact facilities such as hubs, larger facilities, pipelines, transmission hubs and deepwater ports.
Active exercising

The USCG and FBI participate in local port exercises and test multiple response plans simultaneously. Under the current US government regulatory approach the full range of responses to an oil spill, terrorist attack, or hostage situation must be exercised and involve the full range of enforcement and environmental agencies.

Additionally, the USCG as part of their oversight and exercise planning, use independent joint assessments to assess security risks at different locations. Based on these assessments stakeholders agree to implement certain security measures, such as increased radar coverage or the installation of border camera systems, to mitigate identified risks.

In April 2008 the USCG published advice that said that the ability to simultaneously respond and execute multiple security plans (federal, state and local as well as industry response and recovery plans) should be part of an overall exercise and preparedness regime or program. Under these guidance arrangements, federal and other stakeholders conduct exercises that address and deal with an integrated spill and terrorism response.

More broadly, as part of a national exercise scenario program, a training regime has been implemented that exercises all government agencies in a range of 14 crisis situations.

15. Option to test security preparedness:
   – Develop an Australian active exercising program sufficient to test the full range of government and industry responses and that includes a capacity to test the ability to respond simultaneously to multiple security incidents.

Training and awareness

Two US studies in 2010 determined that understanding ‘network risks’ helps to understand the likely multiplying consequences of a deliberate attack on a facility or of simultaneous attacks on several facilities. As an example, knowing the damage that a malicious disgruntled insider could achieve by exploiting vulnerabilities in a production or distribution network offers opportunities to improve the resilience of the network in the most cost-efficient manner.

The National Commission on the BP Deepwater Horizon incident found that examining networks or systems from a safety or engineering perspective may improve knowledge on the way in which individual facilities interact and link with broader systems. The commission’s report examined the roles that industry and government agencies played in assessing vulnerabilities, and the impact of an incident on economic, social and environmental systems. There was a strong opinion that a thorough knowledge of the vulnerabilities of facility and infrastructure networks would help reduce the likelihood of being unprepared for a potential attack or serious incident.

Within the US environment, government is recognised as having responsibility to provide preventive and preparedness guidance to industry and to set standards that minimise risks and ensure compliance. It is expected that government will assess and understand the potential consequences and provide an effective integrated response to an incident sufficient to protect public safety and the environment, to investigate the incident and to assist the restoration of operations in a timely manner.
Annual reviews are also conducted to oversee training programs and compliance standards. GAO is concerned, however, that there is currently no quality assurance assessment of training programs or competencies achieved. Training program content and the identification of desired competencies presently rests with the company and is seen as an industry responsibility. Consequently, standards may vary significantly and will depend upon how seriously a company takes its security responsibilities. A similar variability in training programs and standards was also identified in the Australian offshore environment.

The USCG conducts its own training programs for coastguard personnel at its Virginia College in Yorktown and these may include industry involvement and input.

The USCG Marine Inspection and Investigation School has responsibility for entry and advanced level training for all USCG officers. The USCG has developed a comprehensive set of guidelines known as the Personal Qualification Standard (PQS) which aims, inter alia, to provide advice to USCG personnel about what and how to inspect offshore facilities.

In addition to the PQS, all USCG inspectors are qualified as a Certified Protection Professional (CPP) through undertaking a CPP course that provides a formal licensed security qualification for all USCG investigations and inspection staff. The CPP covers eight major areas of security management: security principles and practices, business principles and practices, legal aspects (US only), personnel security, physical security; information security, crisis management, and investigations. There are two specialty certifications provided under the CPP: the Professional Certified Investigator (PCI) and the Physical Security Professional (PSP).

Similarly, some US-based companies conduct security management seminars and training programs, with training provided on offshore facilities and including face-to-face and online computer-based case management. Some also conduct ‘pre-audit’ audits to prepare for USCG and internal audit inspections. These audits include training components that identify what needs to be done to achieve effective security and how this may be achieved. Many company audits are conducted by security personnel who may work for the company but not the particular facility.

A number of companies also conduct robust drills and exercises involving senior executives as ‘primary incident commanders’. These may run for two to three days, and include lessons-learned style reviews to comprehensively assess the implications arising from incidents that have occurred. Some of these may be joint industry–government reviews.

For example, the OSAC conducted a review of incidents that occurred in Libya at the time of the uprising against Gadaffi. It tested not only the direct security of staff, but also grassroots practical issues such as the maintenance of basic phone communications (phone connection, overload or breakdown issues), safe-haven accommodation options (capacity and location), aviation capacity (evacuation options), provisions and supply options.

As industry security preparedness and efficiency continues to improve, increased integration is occurring between safety and security issues and challenges. In particular, a number of companies are addressing potential safety and security ‘collision points’ in their planning (examples include locked valves for security, unlocked for safety, ladders up versus ladders down, doors locked versus doors open) and defining criteria against which ‘collision point’ decisions should be made.
Case study

The Deepwater Horizon disaster

On 20 April 2010, an unprecedented catastrophic event occurred in the Gulf of Mexico when an explosion occurred aboard Deepwater Horizon, a MODU working on the Macondo Well, about 64 kilometres off the coast of Louisiana.

The explosion and the resulting fire lead to the deaths of 11 personnel, the injury of another 16 and ultimately to the sinking of Deepwater Horizon. Oil gushed unchecked from the uncapped well for 87 days before it was finally shut down.

It was the largest oil spill in the history of US oil production and it caused widespread environmental damage and affected thousands of people whose livelihoods, such as fishing and tourism, are associated with the Gulf of Mexico.

Investigation into the cause of the tragedy began almost immediately and although principally concerned with safety issues, its findings have broader implications that can be extrapolated for the security environment. Especially as there have been moves by some in the industry to combine the responsibilities of safety and security because of their obvious overlaps.

If analysis of the Deepwater Horizon disaster shows anything, it is the devastating cumulative effects of seemingly minor but numerous system deficiencies, acts and omissions, and the failure to respond immediately and decisively to the initial well blow out. Maintenance issues, inoperative alarms and automatic shutdown systems, inadequate training and communication, and the pressure to complete the job, have all been implicated.

The events also highlight the complex interplay of responsibilities of the companies and the government regulatory bodies involved—BP as the designated operator; Transocean, the owner and operator of Deepwater Horizon; Haliburton, who were contracted to BP for the cementing operations; Cameron, who designed the blowout preventer; the USCG and BOEMRE, who carried out inspections on behalf of the US government; and the Republic of Marshall Islands, the flag state for the rig, which delegated responsibility for surveys and audits to the American Bureau of Shipping and Det Norske Veritas. When responsibility is shared among so many, good communication and rigorous auditing and enforcement regimes are essential.

As one BOEMRE report concluded, the Macondo well blowout ‘was the result of a series of decisions that increased risk and a number of actions that failed to fully consider or mitigate those risks’.
North Sea—oil and gas operations

The continental shelf underlying the North Sea is divided into six national sectors, adjoining Belgium, Denmark, Germany, the Netherlands, Norway and the United Kingdom (UK). All, except Belgium, actively exploit the offshore hydrocarbon resources. National legislation and regulation control all exploration and exploitation activities within each sector.

The inquiry team visited facilities and held key meetings in the UK (London and Aberdeen), Norway (Oslo and Stavanger) and France (Lyon and Paris).

All five producing North Sea coastal countries have moved away from highly prescriptive regulatory requirements, toward ‘goal setting’ regimes and a safety-case approach to manage safety and environmental risk. A safety case is a document produced by the operator of a facility that:

- identifies all known and credible hazards and risks;
- describes how the risks are controlled; and
- describes the safety management system.

The descriptions within the safety case must provide evidence that risks are reduced to a level that is ‘as low as reasonably practical’ to ensure industry efficiency and the maintenance of a safe workplace.

The governments of the UK, Norway and Denmark have adopted an ‘all-hazards’ approach where security risk is included in the safety case. The aim of this holistic approach to safety and security is to ensure all hazards and risks are assessed, and minimised or eliminated. How the hazard or risk is caused is immaterial to the safety-case outcome, there are no separate arrangements in place for safety, environment or security, thus ensuring all possible risks to offshore facilities are controlled in an integrated approach.

The European Commission (EC) has published a draft regulation on the safety of offshore oil and gas activities in European waters. The regulations require an approach similar to the safety-case process, but could impose a higher level of obligation on offshore operators than is currently the case with national legislative and regulatory regimes.

The EC considers that the likelihood of a major offshore accident in European waters remains high. In a 2011 communiqué, it identifies that a stringent safety regime and an effective emergency response plan are essential to reduce risk and reduce damage to the environment. Therefore, the EC has proposed a new law to ensure that all European Union regions will respect the world’s highest safety, health and environmental standards for offshore oil and gas production. The regulation will cover the whole lifecycle of all exploration and production activities, from design to the final removal of an oil or gas installation. In addition, European industry will, under control of national regulatory authorities, be required to improve safety standards on a regular basis, taking into account new technology, new know-how and new risks. This new approach, with a risk assessment that continually upgrades, will also include effective prevention of, and response to, a major accident, including a security incident.
For the Mediterranean Sea, recognised as particularly vulnerable due to its semi-closed configuration and significant seismic activity, the EC has developed a proposal for better protection. In this proposal, the European Union (EU) would concede to a Protocol of the Barcelona Convention that protects the Mediterranean against pollution from offshore exploration and exploitation activities. In particular, the protocol requires that construction of platforms and rigs must respect international standards and practice, that operators must prove that they have the technical competence and the financial capacity to carry out the activities, and that damage to existing pipelines and cables will be avoided. The protocol also provides for liability and compensation requirements, and that activities likely to cause significant adverse effects on the environment not be given approval. \(^{14}\)

North and Central North Sea oil and gas facilities map\(^{15}\)

Southern North Sea oil and gas facilities map\(^{16}\)
Countries and their agencies visited by the inquiry team

United Kingdom

As one of the largest producers of offshore oil and gas in the world, the UK employs about 19,000 people on offshore facilities and another 260,000 people in the offshore-dependent sector. The remaining UK reserves of offshore oil and gas are estimated to be equivalent to those it has already produced. Therefore, any interruption to the industry could have a significant financial impact on the UK economy.

After the July 1988 explosion and fire on the Piper Alpha platform that killed 167 people, the UK government made several changes to improve the control of major hazards offshore. It accepted all 106 recommendations made by the Cullen inquiry into the incident and moved the responsibility for the regulation of the offshore industry to the, then newly created, Health and Safety Executive (HSE). The government also replaced the pre-existing suite of regulations (so-called prescriptive regulations because they set specific requirements on duty holders) with new, goal-setting regulations.

In the UK, three authorities are responsible for offshore regulation: the HSE has responsibility for safety, the Department of Energy and Climate Change (DECC) oversees environmental compliance and leak containment, and the Maritime and Coastguard Agency (MCA) responds to pollution from shipping and offshore installations.

The corner stone of the current regime is the creation of a safety case for each installation that demonstrates how a facility will respond and manage a major accident or hazard. The HSE must accept the safety case before the facility can operate on the UK continental shelf.

Regulatory functions, undertaken by HSE’s Offshore Division, include:

- visits to offshore installations to inspect activities on, and in connection with, the installation;
- investigation of incidents and complaints;
- assessment of safety cases; and
- the provision of advice, guidance and technical information.

Every operator or owner of an offshore installation located in the UK sector of the North Sea or the Atlantic margin must have a safety case in place.

In the UK offshore environment, the regulations directly associated with the safety case are the:

- Offshore Installations (Safety Case) Regulations 2005;
- Prevention of Fire and Explosion and Emergency Response Regulations;
- Management and Administration Regulations;
- Design and Construction Regulations; and

The Grampian Police

From a security perspective, the Grampian Police force serves north-east Scotland and parts of the North Sea, giving them responsibility for policing the oil and gas platforms in their area of operation. They are the lead police force in the UK with responsibility for oil and gas infrastructure and undertake regular security exercises to test response and recovery measures with the offshore oil and gas industry.
About twenty officers are trained as Police Liaison Officers (PLOs) and are deployed in company emergency-response control rooms to provide liaison between the company and the police command and control centres in the event of an emergency.

Grampian police officers complete a Basic Offshore Safety Induction and Emergency Training (BOSIET) program aimed at providing officers with awareness of evacuation and fire training responses and participate in regular familiarisation visits to offshore facilities.

An example of good industry to government communication is the secondment of an industry liaison officer to the Grampian Police force. The liaison officer provides an industry perspective, observes the operation of the police emergency response centre, assists in improving interagency coordination arrangements, and also plays an education role within industry to ensure they value and understand the role of the PLOs. The industry liaison officer is currently supplied and funded by Shell on a full-time secondment basis.

16. Option to improve offshore facility awareness and industry-government communication:

- Implement an offshore safety induction and emergency training program similar to that operated by the Grampian Police which provides for deployment of relevant police to industry emergency and response control rooms and on offshore production facilities, as part of a regular familiarisation and liaison program.

\textit{Emergency Preparedness Offshore Liaison Group}

The Emergency Preparedness Offshore Liaison (EPOL) Group is an industry-led forum of more than 30 oil and gas companies that is supported by the Grampian Police force, the MCA and Oil and Gas UK. The group’s aim is to improve offshore emergency response in the northern UK Continental Shelf and West of Shetland.\footnote{18}

In December 2010, the EPOL group backed an exercise for a major oil and gas emergency incident, called Exercise Glass, involving a gas leak and subsequent explosion on the Shell Shearwater Platform. Exercise Glass was conducted by the Grampian Police force and industry, and aimed to test emergency response in the event of a large-scale incident in the North Sea. At the same time the exercise also tested the incident response arrangements under a Memorandum of Understanding between the Grampian Police and the Rogaland Police from Norway, who were invited to attend. Other non-participating members of the EPOL Group were also invited to attend as observers in the various response rooms. Exercise Glass was especially designed to test response times and response capabilities of operators, contractors and emergency services, and evacuation reception centres. The exercise was also filmed and produced an educational DVD.\footnote{19}

In the North Sea environment, active on-site exercising on offshore facilities is recognised as an important contributor to the maintenance of necessary and effective levels of security preparedness and capacity, despite the costs and logistical difficulties involved.
State of Service Representative for Maritime Salvage and Intervention

The overriding authority for incident response from the UK side of the North Sea rests with the State of Service Representative for Maritime Salvage and Intervention (SOSREP). SOSREP, which is essentially a single-person authority, has the widest ranging powers of any government authority identified during the Inquiry process.

The SOSREP is a direct ministerial appointment with support provided by the MCA and has the authority to make all decisions during an operational response, backed by the UK government. There is no authority above the SOSREP and the only method to overturn a SOSREP’s decision is through formal dismissal of the SOSREP.

The SOSREP has the power to:

• take over command of vessels (government and industry);
• direct vessel routes;
• stop port departures;
• destroy assets including offshore rigs, pipelines and fields, and vessels as deemed necessary; and
• shut down the operations of an offshore installation, pipeline and field.

While counter-terrorism responses would be led by the police and military, the SOSREP has the ability to delegate powers to these services as needed and has the ability to exercise partial control of an incident response or total authority if needed.

The SOSREP usually monitors the response to ensure it is in the best interest of the UK. A small team provides support to the SOSREP and will usually consist of:

• a deputy, located in Aberdeen (co-located within the DECC, liaising with oil and gas companies);
• two regional directors involved in interventions;
• an additional member co-located with the MCA; and
• resources provided by the MCA, Department for Transport and DECC.

More broadly, a range of government agencies and bodies collectively share responsibility for the oversight and safe operation of UK-related oil and gas operations in the North Sea.

National Maritime Information Centre

The National Maritime Information Centre (NMIC) operates as a national control centre with responsibility to assist in the protection of the UK interests at sea, including oil and gas production security and maritime piracy.

The NMIC is based at the national military control centre at Northwood in London and is primarily responsible for targeting terrorism and other crime, and assisting the response to disasters. The key function of the NMIC is to facilitate the effective sharing of information in order to maximise the ability to identify and counter potential threats to the UK at an early stage.
**Maritime and Coastguard Agency**

The Maritime and Coastguard Agency (MCA) is responsible for UK maritime policy and the coastguard system. The MCA provides a 24/7 maritime search and rescue service around the UK coast and in the UK International search and rescue region, and also has a range of other responsibilities. These include ship registration and regulation, protection of the marine environment, life saving at sea and representing UK maritime interests at international forum such as the International Maritime Organization (IMO).

The MCA's ship regulation activities include the development, maintenance and enforcement of standards for vessels of all sizes and purposes, including inspections and surveys to ensure these meet UK and international safety rules. The MCA also regulates all commercially-operating maritime qualification and manning activities. In addition, the MCA does real-time tracking and monitoring of shipping movements along the UK coastline and EEZ waters from the shore using an Automatic Identification System (AIS) network around the UK coast.  

**Centre for the Protection of National Security**

The Centre for the Protection of National Security (CPNI) provides protective security advice aimed at reducing the vulnerability of critical national infrastructure to national security threats such as terrorism and espionage. It has no regulatory role.

The national infrastructure comprises the facilities, systems, sites and networks necessary for the delivery of the essential services including: food, communications, transport, energy, water, health, emergency sectors, finance and government.

The CPNI works with government departments responsible for infrastructure sectors; businesses and organisations that own or operate national infrastructure; and other security specialists and advice delivery partners including police. CPNI has a close working relationship and liaison role with government.  

CPNI have a website that enables industry to log on and monitor threat levels and obtain access to publications. Notifications are sent out to industry each time a new publication or threat level assessment is uploaded. Access to the website is by way of secure individual log on, and is not a publically available source. CPNI will grant access to industry representatives based on the CPNI’s determination of need for access.

**Department of Energy and Climate Change**

The U.K. Government’s Department of Energy and Climate Change (DECC) is responsible for all aspects of U.K. energy policy and for tackling global climate change on behalf of the UK DECC was created in October 2008, to bring responsibility for these two policy areas under one department.

The DECC, through its Energy Development Unit (EDU), is responsible for licensing exploration and regulating development of the U.K.'s oil and gas resources. EDU is based in two sites in the UK: London and Aberdeen.
**Health and Safety Executive**

The Health and Safety Executive (HSE) inspects each offshore installation annually and charges industry a set fee per inspection.

HSE inspectors use industry helicopters to travel to offshore installations and can present at heliports and demand a flight. Companies provide HSE inspectors with meals and accommodation while offshore and inspectors (restricted to two or three) are onboard each installation for a minimum of two days.

The inspectors pay particular attention to fire, gas, drilling, pipelines and operational processes.

The HSE has responsibility for the safety-case regime and day-to-day oversight. They provide industry with a set agenda that advises what they are going to inspect.

The HSE have the power to issue a prohibition notice and shutdown operations immediately if they identify an issue that could cause the loss of lives or injury during an inspection. The company must prove that the issues have been dealt with to restart operations. Generally, corrective notices provide time to fix the problems rather than ordering an immediate shutdown.

The majority of HSE officers are technically qualified (engineers and the like) with lengthy experience within the HSE environment. They work closely with the EPOL in the review and assessment of the effectiveness of safety case standards and the continuous improvement of safety effectiveness. There is currently no specific security component within HSE assessments.

**Oil and Gas UK**

Oil and Gas UK is the leading representative body for the UK offshore oil and gas industry. Besides its advocacy role, Oil and Gas UK publishes guidelines to industry.

In February 2010, Oil and Gas UK updated its Guidelines for the Management of Competence and Training in Emergency Response for Offshore Installations. The document outlines best practice in the offshore oil and gas industry for dealing effectively with emergency situations and recommends the training required to develop, demonstrate and maintain the competence of emergency responders. Also in 2010, Oil and Gas UK updated its Guidelines for the Management of Emergency Response for Offshore Installations which provide guidance for duty holders and those parties they need to consult and/or cooperate with when developing or assessing their emergency response arrangements.

The *Guidelines for the Management of Aviation Operations*, which were updated to April 2012, have a particular relevance for the Australian operating environment. The guidelines focus on outbound passenger and baggage security controls at airports and heliports.

Within the UK, heliport security includes identity checks, baggage checks and departure security. The only valid identity document for offshore travel is a valid passport and this is also checked against the confirmed passengers manifest. Baggage is weighed and taken to security control for inspection and manual search in the presence of the owner. It is then moved to a secure area by security personnel and loaded onto the helicopter by authorised ground staff.

Prior to entering secure areas, travellers are subject to a body screening process. Once passengers have entered the secure zone, they are not permitted to leave the area. If they do, they must return through the full security process. Prior to boarding the helicopter, there is a secondary name check and head count against the manifest.
International Association of Oil and Gas Producers

The International Association of Oil and Gas Producers (OGP) is a global industry forum in which members identify and share best practices to achieve improvements in every aspect of health, safety, the environment, security, social responsibility, engineering and operations.

OGP encompasses most of the world’s leading publicly-traded, private and state-owned oil & gas companies, industry associations and major upstream service companies. OGP members produce more than half the world’s oil and about one third of its gas.  

Within the OGP, a dedicated security committee was established three years ago with a direct aim of dealing with issues surrounding offshore infrastructure security across the EU.

The security committee are currently developing guidelines aimed at producing practical solutions to external security risks, covering drilling, production, supply chain and work at sea. Many of the OGP member companies have assets in other parts of the world and the guidelines will include advice on all possible locations (e.g. the North Sea, Indonesia and East Africa).

An essential part of OGP’s mission is to represent the interests of the upstream industry before international regulators and legislators. From its headquarters in London, OGP represents the industry in such UN bodies as the International Maritime Organization (IMO) and the Commission for Sustainable Development and the European Union.

Operators Co-operative Emergency Services

The Operators Co-operative Emergency Services (OCES) is the organisational framework under which oil and gas companies operating in the waters of the North Sea and adjacent waters of the North West European Continental Shelf cooperate and share resources in the event of an emergency situation. The organisation operates along similar lines to the US MWCC and Australia’s AMOSC.

Oil Companies International Marine Forum

The Oil Companies International Marine Forum (OCIMF) is a voluntary association of oil companies with an interest in the shipment, processing and storage of crude oil and oil products. Their goal is to become an authority on the safe and environmentally responsible operation of oil tankers and terminals and to promote improvement in the design and operation of vessels and facilities.

OCIMF have developed risk assessment tools as part of their Tanker Management and Self Assessment version 2, Best Practice Guide for Vessel Operations. The latest version is in draft form and includes shore-based management and ship-based controls for maritime security.

Society of International Gas Tanker and Terminal Operators

The Society of International Gas Tanker and Terminal Operators (SIGTTO) was established to enhance the safety and operational reliability of gas tankers and terminals. It provides a forum for those involved in the industry to share experiences, address common problems and agree criteria for best practices and standards.

SIGTTO publishes studies and produces information papers and works of reference for the guidance of industry members. It maintains working relationships with other industry bodies and government agencies, including the International Maritime Organisation (a United Nations agency) to better promote the safety and integrity of gas transportation and storage schemes.
The OCIMF and SIGTTO assessments and information papers mentioned above offer useful guidance for oil and gas operators operating within Australian waters.

**Norway**

The petroleum industry is Norway’s largest industry. In 2006 Norway was ranked the fifth largest oil exporter, tenth largest oil producer and second-largest gas exporter in the World.29

All offshore and land-based oil and gas infrastructure is classified as Norwegian CI.

Norway has moved from a system of strict regulation and inspections by the Norwegian Government to a self regulated safety-case system. Under this safety-case framework, companies are responsible for the safety and security of everyday operations and are required to put in place crisis management systems. Inspections still occur, but are conducted in an environment where responsibility is placed on the companies. The government inspections are not conducted against a strict check list.

However, at the application stage for the development of an oil and gas field, companies are required to show clear evidence on how they will manage their systems and operations in a safe and secure manner. At this stage, all specifications are required to be clearly outlined. The application document is extremely detailed and is a pre-operational process, which is very closely monitored.

Under this framework, it is industry’s sole responsibility, in a preventive sense, that all operations are conducted safely and securely.

Government investigations and inquiries do occur post-incident. The purpose of these post-incident investigations is to identify what went wrong and develop improvements to current arrangements. Investigations are not conducted to find fault and apportion blame.

**Norwegian Petroleum Directorate**

The Norwegian Petroleum Directorate is a specialist government directorate and administrative body that reports to the Ministry of Petroleum and Energy.

The paramount objective of the NPD is to contribute to creating the greatest possible values for society from the oil and gas activities by means of prudent resource management based on safety, emergency preparedness and safeguarding of the external environment. It has no key responsibility for security.

The NPD have oversight responsibilities from a resource management perspective.30

**Petroleum Safety Authority Norway**

The Petroleum Safety Authority Norway (PSA), created as an independent government regulator on 1 January 2004 is located in Stavanger. Subordinate to the Ministry of Labour, the PSA has regulatory responsibility for safety, emergency preparedness and the working environment in the petroleum sector. This responsibility was taken over from the NPD when the PSA was created.31

While the regulations are safety focused, they do touch on issues relevant to security and the guidelines deal with both safety and security practices relevant to the maintenance of safe and secure business operations.

Essentially, the Norwegian Government stipulates the required standards, but not how to achieve them. The way in which industry achieves those standards and goals is a matter to be determined by them.
The PSA audits list four essential priorities:

- senior management’s capacity to manage—tested at senior management level and with contractors by personnel interview;
- barrier functions—must be tested for effectiveness and management;
- prevention of harm to the environment—including fault and subsea maintenance programs; and
- protection of high-risk operational tasks.

The overall scope of PSA audits is intended to cover the entire oil and gas safety and security environment, including pipelines and onshore facilities.

Approximately 8–10 audits are conducted by the PSA each year. These audits are tightly targeted due to resource restrictions and activities are risk-based and outcome-driven.

Normally, three weeks’ notice is given of the intention to conduct an audit, with industry having an obligation to carry PSA personnel on helicopters to targeted platforms and, if necessary, to offload other passengers to enable this to occur. However, in an emergency, PSA personnel may travel to a platform without notice. Industry bears the cost of supervisory inspections and audits and PSA can advise specific required actions and can intervene and determine what actions a company should take in the circumstances.

Norwegian Police Service

The Norwegian Police Service is a department of the Royal Norwegian Ministry of Justice and Police. The department consists of twenty-seven regional areas and seven national police districts.

The Rogaland Police district, operating out of Stavanger, is close to Norwegian offshore oil and gas facilities and is the primary police district with responsibility for oil and gas infrastructure. Rogaland Police have access to all industry emergency and security plans upon request.

The Norwegian Police lead annual exercises involving the military, police and industry. It is a legislated requirement of the licence issued to oil and gas companies that they must participate in exercises when requested to do so. The exercises are held in a different location each year, but due to high volume of offshore platforms located within the Rogaland Police district, they often occur in this area.

The exercises involve operators and owners of facilities participating in the planning of the security scenario and the exercise. Debriefing is provided for the whole of industry after the exercise is completed.

A unit within the Rogaland Police is specifically trained to establish post-incident crime scene protection on offshore oil and gas platforms after military or armed forces have recovered the platform.

A MOU between the UK’s Grampian Police and the Norwegian Police ensures good communication and information sharing. The Norwegian Police are invited to observe Grampian Police exercises and similar invitations are extended to Grampian Police when the Norwegian Police are conducting exercises in Norwegian waters.

Debriefings occur after the exercises and are held between the PSA, participating companies and the Rogaland Police.
Ministry of Defence

The Ministry of Defence is responsible for the formation and implementation of Norwegian security and defence policy. Regular exercises with the police ensure good coordination between military and police personnel.

The National Defence University conducts two courses each year that focus on national security and safety policy. The courses are attended by government, parliamentary and industry participants, with industry accounting for between 40 and 50 percent of course attendees.

Petroleum Industry Security Alert System

The Petroleum Industry Security Alert System (PISAS) is an industry-funded, continually-manned, security alert system operated on behalf of industry using company representatives on a rotational basis. If an operator identifies an incident, they notify the PISAS centre and the information is relayed to industry. The main centre is located in Stavanger and has proved to be a fast and efficient way to warn all operators or owners of facilities of a security incident. The police and other government authorities have access to PISAS warnings and view these in real time.

Norwegian Oil Industry Association

The Norwegian Oil Industry Association (OLF) is a professional body and employer’s association for oil and supplier companies engaged in the field of exploration and production of oil and gas on the Norwegian Continental Shelf. The OLF works to solve common challenges for the members and to strengthen the competitiveness of the Shelf. OLF has approximately 100 member companies and close ties to Oil and Gas UK.

Within the OLF, a dedicated security committee has been established, attendees of which must be a permanent employee of an operator and must have appropriate security clearances.

OLF runs regular briefing sessions for its members and encourages them all to attend the same session to ensure that they all receive the same information.

The Norwegian Police provide training on how to conduct threat assessments, including improvised explosive device training and crime scene protection, through OLF twice a year. Each course has between 10–15 participants. The course was established about eight years ago and is modelled on a course developed by the Grampian Police.

Oil Security Committee Norway

The Oil Security Committee Norway (OCSC-N), a combined industry and government liaison body, has an oversight security role and functionality similar to Australia’s Oil and Gas Security Forum.

The OCSC-N meets twice a year to discuss security challenges, update threat assessments, discuss police and industry cooperation challenges, as well as providing relevant agencies with specific briefings as required.
Inquiry observations and options for Australia

Protection against armed attacks and other high-threat situations

The OGP has developed guidelines to manage armed attacks on marine operations in exploration and production that deal with external security risks, drilling, production, work at sea and supply.

OGP emphasised the importance of understanding the different types of threats posed to fixed and transient infrastructure, such as oil and gas facilities and maritime shipping.

The guidelines are designed to give managers a good understanding of offshore oil and gas security and help with company security assessments. It has examples of good security measures and gaps and weaknesses to be avoided.

Many multinational companies have in place a range of sophisticated approaches to security risk mitigation and protection. This includes contractors engaged to undertake specialist contractual security arrangements in support of company security activities.

In some locations, such as off the coast of Africa, where the level of threat is seen as higher, they operate a multi-tiered approach to security that is targeted to the perceived risks of that specific location. This includes the use of skilled negotiators in hostage situations.

Some international operators recognise that ‘concentric defences’ are critical to effective prevention and mitigation in locations of higher risk. Such an approach involves a combination of a long-range protective circle (of up to 15 nautical miles); physical protection to the rig or facility, including the construction of a secure citadel; consideration of armed presence onboard; dedicated surveillance operatives; and onboard negotiation expertise sufficient to deal with a likely threat. However, the engagement of armed security onboard facilities in high-threat situations is an extreme last resort and is avoided where possible.

Some companies operating in the North Sea area have clearly defined weapon and munitions management policies that identify the conditions under which anyone (including police) will be allowed to carry and/or store weapons on board a facility. A specific concern of the oil and gas industry is that government responders do not have a sufficient understanding of the safety issues involved with the carriage of weapons on board oil and gas infrastructure.

A first step in maintaining security around an asset is to provide the earliest possible notice of an impending threat and delay any attempted incursion to allow employees time to reach the citadel. There are many types of detection systems available and some can identify potential threats from large distances. However, the costs associated with the maintenance of the equipment and the training of employees can be high. Long-range CCTV can cost between $250,000 and $350,000 and may include continual update costs such as calibration.

Protection plates on anchor lines and other hawser lines and hoses that provide potential points of access may be difficult to install, but are also difficult to overcome. The retrofitting of such preventive barriers, including barbed wire and anti-grip paint, is increasingly occurring on rigs or facilities prior to their transport to a drilling or production location.

In broader terms, security is increasingly being taken into account during the budget and design phase of offshore facilities. In the international environment, acceptable security costs are generally between 2–4 per cent, but in particularly dangerous locations they can be between 15–25 per cent and in some cases as high as 40 per cent.
There is recognition that oil and gas companies must clearly define the security responsibilities of contractors prior to doing business, including the steps necessary in response to an incident. A document and legal framework between contractors and oil and gas companies that identifies the chain of responsibility and liability for security issues is an important part of defining the responsibilities of both parties. This has direct relevance in the Australian offshore oil and gas sector where currently limited security obligations are placed on contractors and subcontractors.

The Vantage POB Tracking System is a Person on Board internet based tracking tool that is widely used by oil companies, drilling companies and helicopter operators in UK waters and increasingly used for offshore work in Ireland, Denmark and the Netherlands.

The system has been introduced as an aid to improving offshore safety using a web-based system which enables users to efficiently monitor and control the movements of personnel to and from offshore facilities and also onshore sites such as process plants.

Additionally, by providing a central recording system, it helps remove the need for duplicate training when moving between offshore assets of different offshore operators and countries. Vantage POB holds up to date information on an offshore workers’ survival training records, medical certificates, e.g. expiry date, trip history, and offshore facility/helicopter inductions. In the future it may hold details of other important competencies.

This provides an electronic safety filter to ensure everyone travelling offshore has successfully completed the proper training and provides offshore operators with enhanced safety, security and operational efficiency.

Additionally, the Vantage tracking system holds details of persons to contact in case of an emergency.33

In a number of countries, essentially those with emerging economies, oil and gas companies often provide local authorities with boats, training, and meet the costs of the security patrols provided by government organisations.

In May 2000 BP announced Project Jigsaw to enhance its North Sea platform safety provision by replacing standby vessels with SAR helicopters. Other elements of the Jigsaw Project include maritime assets, cold weather suits for outside work and the extended use of locator beacons. Another Jigsaw element is the provision of radar early warning systems to provide collision risk protection on several BP installations.

Project Jigsaw uses locator beacons on all helicopters, standby vessels and fast rescue craft, connected to a computer based emergency response system located in Aberdeen. This ensures the locations of all rescue craft and helicopters and their response time are always known to staff in the BP control centre.

On 18 February 2009, a Super Puma Helicopter ditched in the sea whilst approaching one of the North Sea based ETAP offshore installations. All 18 passengers and crew were rescued. BP’s Project Jigsaw is credited with the safe, quick and efficient recovery of the 16 passengers and two crew from the water.34

Industry generally recognises that people, rather than technology, are the most effective preventive mechanism. As a consequence, a number of companies operating in the North Sea have integrated the roles of their security managers and the use of cost-efficient technology as part of their security framework. This technology may include surveillance, including aerial balloons, floating cameras, trip wires, beacons, sensors and radar.
Norway has a crisis management system that is managed by the Government Crisis Council. The council consists of the secretary generals of the relevant ministries, with two representatives attending the council from each ministry. The first agenda item at the initial incident response meeting is to establish the lead response agency. This arrangement is deliberately aimed at avoiding cross-agency or jurisdictional confusion or uncertainty in command and control arrangements.

A Defence Crisis Support Unit provides the liaison between police and defence services as part of the incident management process.

The 22 July 2011 lone-perpetrator attacks in Norway, which resulted in the deaths of 77 people, led to a recognition by government that a single agency needed to be identified to manage responses across ministries to any serious incident.

During this incident defence supported police operations with operational requests made under strict police–defence guidelines that detail individual responsibilities. Ministerial approval is normally required for operational requests, although during the 22 July 2011 incident, approvals were verbal and generally took no longer than 5–10 minutes.

Military and privately owned helicopters may be used in response to an emergency or incident. Exercises are also used to certify helicopters for night and blind landings, and for offshore facility training.

At the time this inquiry team visited, there were 14 ships engaged in Norwegian coast guard duties. All are purpose built and can house helicopters and facilitate helicopter landings, although only some are equipped with helicopters. Coast guard ships in southern Norwegian waters do not ordinarily carry helicopters, as quicker responses can be achieved from land, the oil and gas facilities being closer to shore than further north. Ten of the fourteen ships are usually at sea and operational at any given time.

Shipping within Norwegian and British waters in the North Sea for the passage of cargo ships and supply shipping is seen as a potential security risk. In Norway, the aim of the coast guard is to monitor all tankers transiting Norwegian waters and to push the ships as far out to sea as possible to provide a longer lead time in the event of the need to prevent or respond to a potential incident.

Examples of actual incursions where protestors had boarded offshore platforms and chained themselves to the facilities were provided to the Inquiry team by industry. Experience indicated that protestors usually arrived in small groups of three to four people, but caused major disruptions, as it was necessary to halt drilling while they remained onboard. Protestors were usually well equipped with sophisticated equipment, boats and survivor suits. As well as boarding offshore infrastructure, on occasions protestors had placed themselves in front of the path of a moving rig.

Response to incidents of this nature are ordinarily handled by Norwegian Police, with the industry approach being to contact police, act calmly and politely to protestors and, where possible, move them to the safest possible location on the platforms prior to police arrival.

Intelligence and information on possible protest activity is shared with industry and security managers are briefed on protest response arrangements and provided with a classified specific security plan on the potential protest. All protestors entering exclusion zones or gaining access to assets are charged with a criminal offence.
Each facility has a detailed security plan covering full helicopter offshore operations. These plans cover all helicopter movements to and from heliports and offshore facilities. Some plans are available for distribution and shared between companies and facilities, while others with commercial or sensitive information are classified and remain in-house. Separate safety and security plans are generally prepared to cover different incidents such as collisions, fire, weather emergency or acts of terror.

**Employee and cargo security arrangements**

Benchmark employee and cargo vetting and security arrangements in the North Sea include cargo being sealed prior to loading onto either a supply boat or helicopter, and operator audits on all cargo. Secure tamper-proof sealing of all cargo intended for offshore facilities was identified by government agencies and industry as being of particular importance.

A particular issue of concern identified to the Inquiry was the vetting of crews onboard supply vessels, as supply vessel security is processed and managed by the shipping company.

Security checks are carried out on all employees before starting employment. Security checking is simplified in the Norwegian context because a majority of facility and supply vessel employees are Norwegian, with the balance essentially coming from across broader Europe. Most companies provide their employees with identification cards and have access controls that restrict the employees to their work areas.

With regard to heliport security, Norwegian arrangements generally conform to full aviation-style security screening. These include X-ray; walk-through metal detectors; checking for explosives; checking of passenger identification, travel documentation, work permits and luggage; random personal checks; and cargo screening.

Random checks are also carried out on return flights to minimise the theft and removal of tools, explosives and other items and to ensure that such items being lawfully carried are being packed and handled correctly.

Despite these security arrangements, an example was provided to the Inquiry team of an audit offshore facility where all restricted liquids had been removed from a platform, but where in a second audit several months later, the same restricted liquids in similar quantities were found onboard the facility.

Drug and alcohol use was identified as a major problem and some companies are attempting to initiate a project to check the sewage from offshore platforms for illegal drugs in the system. Cocaine use was raised as a drug of particular concern.
Security preventative measures

In response and resilience terms, major companies operating in the North Sea area were likely to have a range of security preventive measures in place including:

- radar and AIS;
- standby vessels with capacity for AIS class A exchange of data;
- vessel traffic management systems involving:
  - radar information;
  - electronic mapping charts;
  - oil spill detection radar;
  - comprehensive weather data; and
  - facilities for data exchange between offshore and onshore facilities;
- a permanently manned emergency operations centre, comprising:
  - dedicated positions with clear roles and responsibilities;
  - linkages to the PISAS; and
  - backup generator capacity.

These arrangements are an example of leading-edge practices that are worthy of consideration in the Australian offshore environment.

An Interpol perspective

Interpol is not aware of any specific threats against offshore facilities in the North Sea and, because it requires a degree of seamanship to navigate near or around a facility, offshore facilities are not seen as likely targets in comparison to other facilities such as transport hubs. However, this lower likelihood of attack is not seen as a license to ignore offshore infrastructure security.

In the case of an organised criminal incident, such as terrorism, targets are likely to be those where mass casualties would be the result. Continual vigilance, such as the reporting of unusual boat movements near a facility and effective mitigation strategies are seen as fundamental to security, as is the assumption that the conspirators or perpetrators would be educated and well prepared.

Interpol believes the most likely threat to security is from industrial issues or the personal grievances of disgruntled employees and disaffected staff. To this end, stringent background checks on all employees with access to materials or a potentially dangerous environment are seen as particularly important.

Front-end security is also seen as a priority to ensure staff understand the importance of security and are trained and encouraged to report anything they may have heard or become aware of, even if security implications are only minor. This could be the purchase of products such as boats and other items relevant to criminal activity in neighbouring centres.
South-East Asia Meetings—oil and gas operations

The Inquiry team conducted meetings with key government organisations in Indonesia and the Philippines, but did not participate in any site visits.

In Indonesia, the Inquiry team met with representatives of the Ministry of State Enterprises (BPMIGAS), the Deputy for Infrastructure and Logistics, the Ministry of Energy and Mineral Resources, the Indonesian Sea and Coast Guard, and representatives of two companies, BP and SANTOS, which are operating in the region.

In the Philippines, the Inquiry team met with the Philippine Coast Guard and the Philippine National Police.

Countries and their agencies visited by the inquiry team

Indonesia

In 2010, Indonesia’s oil and gas sector contributed approximately $23.3 billion in government revenue. Currently, Indonesian gas production accounts for around 11 per cent of the world’s LNG and is exported to Japan, South Korea, Taiwan, Mexico and China.\(^\text{35}\)

Indonesia’s oil and gas executive agency is BPMIGAS, which supervises oil, gas and LNG production. Its main function is to oversee and control the business activities in accordance with the cooperation contracts with private operators for the extraction of oil and gas in Indonesia.

Indonesia’s offshore oil and gas security is undertaken by the Indonesian Navy and the Indonesian Sea and Coastguard.

Offshore oil and gas security issues of relevance to the Inquiry include the 24-hour incident reporting centre within Jakarta that receives all reports of terrorist and/or other serious incidents occurring in the air, on sea or on land. All reports received are then prioritised by the centre and directed to the appropriate organisation. As part of the arrangements between government and industry, security MOU’s are in place between the offshore oil and gas operators and the Indonesian government agencies. Under these agreements, the Indonesian Navy conducts patrols of the offshore production areas, facilities and pipelines to enforce exclusion zones.
Philippines

As of June 2011, the potential petroleum resources of the Philippines were estimated at 27,905 million barrels of oil and 53,870 billion cubic feet of gas.\(^{36}\)

Exploration and production activities in deepwater areas off the Philippines are increasing with the discovery of new deep-sea oil and gas deposits in the Malampaya Oil Rim and other recent exploration and production activities taking place in the Mindoro, Salawan, and Sulu Sea basins.

The Malampaya Deepwater Gas-to-Power project is the largest natural gas development project in Philippine history, and one of the largest-ever foreign investments in the country. The Malampaya Project holds an estimated 3.7 trillion cubic feet of natural gas reserves. Natural gas from Malampaya is pumped via a 312-mile sub-sea pipeline to a natural gas processing facility and three power plants in Batangas that have a combined generating capacity of 2,700 megawatts.\(^{37}\)

The Philippine Navy, Philippine Coast Guard and the Philippine Maritime Police work closely through MOU arrangements to provide layered security for the offshore oil and gas projects. These agreements lay down the operating procedures between agencies to prevent duplication of effort in areas of overlapping responsibility.\(^{38}\)
Australian oil and gas operations

Production

In 2010–2011, Australia’s oil and gas exports were valued at $25.309 billion. LNG production was at 20 million tonnes and crude oil production at 19,701 million litres. Together the offshore oil and gas industries employ about 20,000 people.39

Australia’s production of petroleum liquids peaked in 2000 and has been steadily declining since. In 2002–03, Australia still had a trade surplus in oil and liquid fuels, but rising demand and falling production have caused a trade deficit in petroleum products of about $16 billion per year since then. Without major new oil and condensate discoveries, this will grow to about $30 billion per year by 2015.

Australia is currently the fifth largest LNG exporter in the world and the industry is developing projects that will make Australia the world’s first or second largest LNG exporter by 2018.

At the same time, Australia’s offshore LNG projects are extending further northwards from Australia, with major developments underway in the JPDA between Australia and Timor Leste and closer to Indonesia.

Australia’s oil-producing regions include Western Australia, the Timor Sea, the Northern Territory, Queensland, Bass Strait and South Australia.

New oil producing projects are under development for the Kipper and Turrum fields in Bass Strait, and the Van Gogh and Pyrenees fields in Western Australia commenced producing oil in 2010.

The country’s first LNG project, the North West Shelf Venture (NWSV), began shipping LNG in 1989. This operation has since grown to include five production units (or trains) and it now produces up to 17 million tons per annum. A second LNG development, Darwin LNG, began production in 2006. This one-train project produces up to 3.5 million tons per annum.

Five large Australian LNG hub developments are currently under construction. Three offshore fields in north Western Australia—Pluto, Gorgon and Prelude—and two land based Coal Seam Gas (CSG) to LNG conversion projects in Queensland, Queensland Curtis and Gladstone LNG.

Pluto LNG will come online in 2012 and will initially have one 4.3 million tonnes per annum production train, although there are plans to add further trains. Gorgon will have three trains producing 15 million tonnes per annum from 2014.
A key factor in the development of the LNG industry in Australia has been the long-standing relationships with major Asian utility companies, who regard Australia as a high-quality supplier. In the last two years, north Asian utilities and gas companies have signed significant LNG supply contracts, underpinning the current development of Australian LNG.
Innovations

Australia is a world leader in LNG innovation and CSG technology.

The Prelude project will be the first use anywhere in the world of a floating LNG (FLNG) processing, storage and offload vessel. The FLNG facility will be located in the remote Browse basin, 475 km north-east of Broome, Western Australia, and will be 488 metres long, 74 metres wide and weigh around 600,000 tonnes when fully loaded.

The Prelude FLNG facility is expected to stay moored for 25 years and produce at least 3.6 million tonnes per annum of LNG as well as LPG and oil condensate for export. The FLNG vessel is under construction and the project is expected to begin production in 2016 or 2017.

The world’s first CSG to LNG conversion projects are being developed in Queensland. CSG found in coal deposits has recently become commercially viable and contributes 90 per cent of Queensland’s domestic gas. CSG in the Surat Basin of southern and central Queensland typically contains more than 98 per cent methane, with very small amounts of nitrogen and carbon dioxide. This means that the CSG requires little treatment before it can be converted to LNG.

Two of these schemes, Queensland Curtis and Gladstone LNG, are currently under construction. Two other large CSG to LNG conversion projects are also being planned for Queensland, although these have not yet finished working their way through the federal and state approvals processes and final investment decisions.

LNG

Offshore LNG projects under construction include Gorgon in the Carnarvon Basin and the Pilbara ($43 billion); Wheatstone in the Carnarvon Basin and the Pilbara ($29 billion) and INPEX in the Browse Basin and Darwin ($25 billion). The Greater Sunrise project in the Timor Sea has a projected value of $14 billion and will use an FLNG offshore processing storage and offload facility.

Current LNG projects and those in development have attracted more than $200 billion in investment and the industry is targeting production of at least 60 million tonnes per annum by 2020. With long term contracts and field viability of up to 25 years, LNG projects will contribute significantly to national, state and territory economies. For example, a typical new LNG project could deliver $40 billion (nominal dollars) in tax and royalties over its lifetime.

Major benefits identified by industry include:

- a potential improvement in the balance of trade in the order of $20 billion a year by 2017 based on a forecast 50 million tonnes per annum production rate;
- a projected reduction of around 180 million tonnes per annum of carbon dioxide equivalent globally by 2017 (equivalent to more than one quarter of Australia’s projected greenhouse gas emissions in 2017);
- a greater energy supply security;
- an increase in revenue to governments; for example, a single new LNG project could generate $40 billion (nominal dollars) in tax and royalties over the life of a typical project;
- a more skilled workforce and an increase in employment in the oil and gas sector and service industries (up to 52,000 new jobs at the construction peak);
- an increase in regional development, particularly in Western Australia, Queensland and the Northern Territory;
• an expected tripling in shipping traffic off the NWS and Timor Sea areas, as LNG and iron ore construction projects enter production phases; and
• an expected four-fold increase in LNG vessel traffic in the above sea areas in the next decade.

In addition, the collective export by the Western Australian iron-ore ports of up to 1 billion tonnes of ore per year, the expansion of general and other cargo operations to support this growth and the anticipated new ventures in extractive industry exports will add to the volume of maritime traffic transiting in the vicinity of current and projected offshore oil and gas infrastructure located off the North-West coast and Timor Sea Areas.

**CSG**

If the eight currently proposed CSG/LNG projects in Queensland proceed, more than 59 million tonnes of LNG will be produced per year as a result of extracting CSG. The CSG from the Surat and Bowen Basins will be sent to the coast, where it will be stored and exported. Seven of the eight projects will use the export facilities on Curtis Island and Fishermans Landing at Gladstone, Central Queensland, while one project will use Abbot Point, near Bowen in North Queensland.\(^42\)

The issue of CSG mining on the Australian mainland, however, remains contentious and is subject to continuing debate and protest, with protesters claiming that the development of CSG will have a range of environmental consequences. While most protesters are law-abiding, there has been some criminal activity, with protesters arrested as a consequence.\(^43\)

The potential threat posed by unlawful protest activity in the onshore environment should not be ignored in the security assessment process.

**The industry position**

The oil and gas industry is essentially risk averse and wants to operate in a secure offshore and onshore environment.

Offshore oil and gas exploration is expensive and risky and development and production require long-term planning and substantial investment.

The majority of oil and gas companies operating in Australian waters are multinational corporations with ventures in other parts of the world. As a result, company safety and security standards and practices tend to reflect a company’s international arrangements, tailored to reflect the perceived threats and risks in the location of operation.

While, understandably, the safety culture within the oil and gas industry is more entrenched and mature than that of security, companies are continually improving their security arrangements and practices. In places such as Africa and the Middle East, security arrangements are especially well developed and, in a number of cases, these arrangements have been actively tested.

Within the Australian environment, security planning is a relatively new priority with Australian-based management positions in company security being only reasonably recently introduced. A number of companies have tailored their international safety and security policies to meet Australian requirements and to the identified threats and risks.
While the larger companies are likely to have well developed security regimes in place, others, with less international or operational experience or with economy-of-scale restrictions, may have less rigorous and comprehensive security programs and face more difficulties in implementing a comprehensive security regime. As a result, the standard of security awareness and preparedness across Australian oil and gas operations is currently variable and will benefit from ongoing engagement with government.

The strong safety culture which exists across both the offshore and the onshore industry is consistently reflected by well-developed procedures, training, drills and exercises. Many of these practices have obvious relevance and application to the security environment. At the same time, to genuinely integrate safety and security regimes, a more balanced and objective assessment of the many safety and security tension points may need to be addressed when determining safety and security priorities and arrangements in a given situation (e.g. valves locked or unlocked, access doors open or locked).

In some companies, safety and security planning and response arrangements have been interconnected. Indeed, the industry security arrangements that appear to be most efficient are those which are integrated with, or closely aligned to, safety arrangements.

The threat scenario

To date, Australia has been consistently considered as a low-risk, location with high security and supply reliability. However, the shape of the oil and gas industry is changing and Australia increasingly has a range of characteristics within its operating environment that are likely to heighten security implications in the future.

As the Australian-based industry and associated employment demands continue to grow, the employee profile of many companies is changing and more foreign workers, generally operating under 457 visa arrangements, are being engaged.

While there is no evidence, apart from the issue of cyber intrusion, of any specific threat against offshore oil and gas infrastructure in Australian waters, there is international recognition that threats to offshore infrastructure do exist. Terrorist groups have indicated an interest in economic targets, including oil and gas tankers and energy-related facilities, and US government authorities have identified that the petroleum industry may be a terrorist target due to the inherent nature of the business and the importance of the industry to the national interest. This assessment has obvious application to Australia.

In terrorist terms, international and Australian assessments indicate that the threat to offshore infrastructure could emanate from home-grown or internationally driven terrorist operations. Methods such as boat-borne explosive devices, armed intrusion (including armed assaults with subsequent placement of explosives), direct attack (stand-off attacks using automatic high-powered weapons, rocket propelled grenades), hijacked vessels and/or aircraft (as kinetic weapon attacks where aircraft or ships are crashed into facilities), sabotage (targeting single points of failure), and underwater attacks are all considered possibilities.

However, based on both government and industry advice and assessment, the risk of terrorist takeover of an offshore facility operating in Australian waters is low, with the much more likely threat seen as coming from a ‘trusted’ or disgruntled insider or a lone intruder.
In terms of insider or intruder based threats, the tragic criminal attacks, allegedly committed by Anders Breivik in Norway on 22 July 2011, provide a dramatic example of the potential of an organised disaffected or unbalanced lone perpetrator. Breivik, apparently operating alone, has admitted carrying out two violent attacks in quick succession against the government, the civilian population and young Norwegians attending a labour party summer camp on Utøya Island near Oslo.

The first attack involved a vehicle bomb, exploded within the executive government quarter of Oslo, which killed eight people and injured at least 209, including 12 seriously.

The bomb used was made from a mixture of easily obtainable and processed fertiliser and fuel oil, which apparently was purchased through the internet under the guise of a business which had been created solely to legitimise the purchase of large quantities of fertiliser.

The second attack which occurred less than two hours later on the Island of Utøya, some 40 kilometres north-west of Oslo, resulted in the deliberate shooting deaths of 69 attendees at a labour youth league camp with at least 110 others receiving injuries.

To access the island Breivik had apparently used false identification papers and a fake police uniform.

For the above reasons, a consideration of the facts and circumstances of the 22 July 2011 ‘Breivik’ incident is relevant to any risk assessment of vulnerabilities in the Australian oil and gas industry security framework.

In the Australian context, apart from the growing numbers of foreign workers engaged in the industry, many Australian based workers operate on a ‘Fly-In, Fly-Out’ (FIFO)—or in the Queensland CSG environment a ‘Drive-In, Drive-Out’ (DIDO)—basis. As a consequence, many workers are engaged on rotational rosters that combine two, three or six week (or similar) on-site work periods with significant periods of ‘off duty’ or recreational time (e.g. two weeks on, two weeks off).

Workers frequently reside many hundreds of kilometres away from their work site and, those who have partners and families spend long periods of time away from their family environment. As in any work situation, this combination has the potential to be a cause of discontent and frustration that needs to be understood when assessing security issues and risks.

Reinforcing these concerns, the inquiry into the use of FIFO and DIDO workforce practices in regional Australia by the Federal Parliamentary Standing Committee on Regional Australia has heard medical evidence of high rates of mental illness and serious drug and alcohol problems within the workforce. These issues can only increase the potential for unstable and unpredictable employee conduct.

As is the case internationally, the ability to effectively vet potential employees, either through company recruitment processes, MSICs, passport or 457 visa related checks is essentially limited to basic character style assessment and cannot operate as a genuine security clearance process. These limitations need to be understood and reflected in other and wider complementary security arrangements.

Many issues can give rise to workplace discontentment. A worker who has been involved in a domestic altercation immediately prior to returning to the workplace; a worker who has a drug or alcohol problem; a worker who is chastised or threatened with dismissal by a supervisor or a worker who loses significant money in a card game, can each quickly change from a trusted and reliable employee to a disgruntled or disaffected employee and a potential security risk.
The continued expansion of the Australian LNG industry also makes it likely that there will be an increase in foreign flagged and owned vessels in Australian waters. These vessels will be crewed, in increasing numbers, by foreign seafarers, many of whom may not be subject to any Australian-based employment vetting or assessment process.

On some facilities located in northern Western Australian waters and in the JPDA, a particular threat is potentially posed by the crews and passengers of Suspected Illegal Entry Vessels (SIEVS) and by international fishing boats operating close to, or approaching, offshore facilities.

The Australian offshore oil and gas industry is continuing to expand exploration further offshore in the search for new oil and gas fields. At the same time, technology developments and other innovations are increasingly reducing operational costs and enabling deepwater production to become more viable.

The improvements in technology are increasing the ability of offshore production facilities to operate without crews. Such facilities, together with connected subsea well installations, are being operated by Supervisory Control and Data Acquisition (SCADA) - type control systems, which are frequently located hundreds of kilometres from the actual operational site. Whilst these computer-monitored unmanned facilities are highly cost efficient, they carry additional risks, are open to an increased threat from cybercrime and cyber intrusion, and provide new opportunities for sabotage, supply disruption and commercial damage.

Indeed, despite the tendency to emphasise the threat from physical terrorist or criminal activity, cyber attack is probably already the most serious threat to the integrity of offshore facilities and land-based production. Hence, cyber security is the most important future challenge for oil and gas facility operators.

However, the primary focus of this report is the matrix of security oversight and incident preparedness and response.

**Agencies visited by the inquiry team**

In Australia, the inquiry team conducted a comprehensive series of meetings with government and industry representatives and made site visits to 31 offshore and onshore facilities. The aim was to gain an understanding of the security arrangements in place and the methodology adopted by various companies. The site visits also allowed the inquiry team to compare and contrast the Australian working environment, and related security measures, with international practice. See Appendix 3 for a complete list of meetings and site visits.

**Government**

Within Australia’s federal environment, a number of Australian Government and state or territory government agencies have a role in the regulation or oversight of the offshore oil and gas, and related maritime, environment. The responsibility for security related oversight, regulation and response is essentially shared between the ADF, BPC, OTS and state and territory police.

**Border Protection Command**

The Border Protection Command (BPC) is a multi-agency command comprising representatives of the Australian Customs and Border Protection Services, the Department of Defence, the Australian Fisheries Management Authority, and the Australian Quarantine and Inspection Service.
This interagency structure aims to maximise the efficiency of maritime security, surveillance and response coordination through using maritime-related information from all sectors of Australian Government and the targeted deployment of military and civil assets. As part of this process BPC manages the Australian Maritime Identification System (AMIS), which draws together all maritime information collected across government to produce a single, comprehensive, whole of government awareness picture of Australia’s maritime domain.

BPC is the primary government law enforcement organisation in the Australian maritime domain and enforces legislation that covers the territorial sea, the contiguous zone, the EEZ and the continental shelf. It also enforces the protected areas and protected zones. In addition, BPC is also Australia’s Security Forces Authority for the purposes of responding to acts of violence against ships within the Australian Search and Rescue Region.44

In the performance of these responsibilities, BPC utilises aviation and maritime surveillance and response assets provided by the ADF and the Customs and Border Protection Service. These assets currently include Royal Australian Navy patrol boats, Australian Customs vessels, Royal Australian Air Force Orion maritime patrol aircraft, Army Regional Force surveillance units and contracted Coastwatch aircraft and vessels.

**Office of Transport Security**

The Office of Transport Security (OTS) forms part of the Department of Infrastructure and Transport. The OTS works with the states and territories, other government agencies, international governments and bodies, and the aviation and maritime industry to improve security and prevent transport security incidents. Its activities include transport security intelligence, transport operations, and transport security policy, planning and regulation. In addition, it is also involved in auditing of compliance and security measures, and in ensuring that a nationally consistent approach is taken and that Australia’s transport security arrangements comply with international standards.45

As part of this mandate, OTS has responsibility for regulating aviation and maritime security under both ATSA and MTOFSA requirements. This involves OTS approving aviation and maritime security plans and conducting on-site audits and inspections of RPT aviation security activity (including oversight of ASIC and screening processes) and of regulated maritime ports and shipping (including oversight of MSIC, cruise-ship screening processes and tanker security operations). In accordance with the current risk context assessment for the security of offshore production facilities, the security plans for offshore production facilities are only subject to desktop audit and assessment approval.

**Police forces**

The role of state and territory policing in terms of security for offshore oil and gas facilities is more clearly defined than that of the Australian Federal Police (AFP). While to date no Australian police force has dedicated resources solely to the offshore oil and gas industry, police in Victoria and Western Australia work closely with the industry and are involved in periodic active exercises on offshore facilities. Their resources are, however, unavoidably limited, and their oil and gas responsibilities are combined with wider law-enforcement responsibilities within their region of operation. In oil-relevant coastal jurisdictions, their capacity to respond to incidents, which may occur some distances offshore, is restricted and, in some cases, may be non-existent.
Much of the offshore oil and gas infrastructure is located in the north and north-west of Australia where population density is low. Communities in these areas are generally small, are often separated by significant distance and are supported by police operating from regional centres, with large areas of geographic responsibility and limited human resources and assets.

The responsibilities of the AFP are less clearly defined. The arrangements for federal, state and territory police cooperation and response to a terrorist incident, under National Counter Terrorism Committee (NCTC), are well understood, however, the situation is less clear if the cause of an incident is either unknown or clearly of a criminal nature. In these situations, the primary initial response may well fall solely on the police force of the relevant state or territory jurisdiction.

The AFP does not have a permanent presence in the north and north-west of Australia outside Darwin. Although the AFP has jurisdiction to investigate counter terrorism, human trafficking and sexual servitude, and cyber crime cases, in other situations the AFP does require agreement with the relevant state or territory before it has authority to exercise in a particular state or territory jurisdiction. Similarly, apart from the provision of community-policing style services in the Australian Capital Territory, Jervis Bay and identified external territories, the AFP has no direct responsibility to police breaches of state or territory law in Australia or Australian waters.

The *Australian Federal Police Act 1979* (Cth) specifically addresses the complex, and potentially difficult issue, of when AFP officers have authority in relation to offences against state or territory laws. The Act identifies state and territory offences that have a federal aspect, either because of the elements of the offence or because of the circumstances in which the offence is committed.

Similarly, defence force aid to the civil power may be more difficult to determine where an incident appears to be of a purely criminal nature.

While the ADF works closely with BPC with regard to offshore protection matters and is responsible for the offshore counter terrorism domain, land based counter terrorism response and criminal incidents are primarily police responsibilities in which the ADF provide assistance as requested.

Australian police and emergency services exercise the same jurisdiction over visiting ships as they do in their onshore work. Foreign-flagged vessels visiting Australian ports are subject to Australian law, as are Australian ships.

**Computer Emergency Response Team**

The Commonwealth’s Computer Emergency Response Team (CERT) is the initial point of contact for cyber security attacks on networks in Australia. CERT also works with the private sector to identify critical infrastructure and systems and provides information and help to protect information technology infrastructures.46

**Cyber Security Operations Centre**

The Cyber Security Operations Centre (CSOC) was established in the Defence Signals Directorate to mitigate cyber threat to Australia’s national security. The organisation provides the Australian Government with information about emerging cyber threats against Australian interests and coordinates and helps in operational responses to these threats.47

In the area of offshore oil and gas business continuity, economic competitiveness, safety and the environment, a number of Australian government agencies also share responsibility.
Department of Resources, Energy and Tourism

The main role of the Department of Resources, Energy and Tourism (DRET) is to ensure that Australia maintains its international competitiveness when responding to the increasing globalisation and technology developments of the resources, energy and tourism industries. DRET liaises closely with the private sector through major corporations and business associations.

On 1 January 2012, two new branches of DRET’s Resource Division started operating. These include the National Offshore Petroleum Titles Administrator (NOPTA) and the expanded National Offshore Petroleum Safety and Environmental Management Authority.

National Offshore Petroleum Safety and Environmental Management Authority

The National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) is Australia’s first national regulator for health and safety, well integrity and environmental management of offshore oil and gas operations. This responsibility, which previously rested with designated state and territory authorities, was passed on to NOPSEMA through the Offshore Petroleum and Greenhouse Gas Storage Amendment (National Regulator) Bill 2011, following recommendations arising from the Final Government Response to the Report of the Montara Commission of Inquiry (2011) and the Productivity Commission Report (2009).

NOPSEMA replaces the National Offshore Petroleum Safety Authority (NOPSA), established in 2005, which aimed to regulate the health and safety of workers on offshore facilities in Commonwealth waters, and in waters where state powers had been conferred.

NOPSEMA’s is responsible for the regulation of occupational health and safety, wells and well operations, together with regulation of the structural integrity of facilities and environmental management within Commonwealth waters. This amalgamation of safety, well management regulation, integrity and environmental management responsibilities into a single regulator is expected to reduce the regulatory burden on industry. It will also standardise Australia’s offshore petroleum regulation to a quality, best practice model.

Australian Maritime Safety Authority

The Australian Maritime Safety Authority (AMSA) is a largely self-funded government agency that aims to enhance the efficiency of how safety and other services are delivered to the Australian maritime industry. The authority is responsible for marine environmental protection, search and rescue, shipping safety and marine pollution response training.

AMSA’s search and rescue service covers over some 52.8 million square kilometres of the Indian, Pacific and Southern Oceans and is delivered by the Rescue Coordination Centre-Australia.

To meet requirements for safety and protection of the maritime environment, AMSA undertakes vessel tracking and coastal traffic management measures using ship-based AIS and Long Range Identification and Tracking (LRIT). This is used in programs such as the Great Barrier Reef –Vessel Traffic Management System and the Vessel Tracking program.

AMSA also manages The National Plan to Combat Pollution of the Sea by Oil and Other Hazardous and Noxious Substances, which aims to maximise Australia’s marine pollution response capability. This plan is a cooperative arrangement between AMSA, the states, the Northern Territory and the petroleum, chemical and shipping industries.
Industry

Australian Petroleum Production and Exploration Association

The Australian Petroleum Production and Exploration Association (APPEA) is the peak national body representing Australia’s oil and gas exploration and production industry. APPEA represents over 80 full members and 220 associate members. The full members include the oil and gas exploring and producing companies, which together account for an estimated 98 per cent of Australia’s petroleum production. The associate members of APPEA include those companies that provide goods and services to the oil and gas industry.

APPEA’s main focus is to secure conditions that enable member companies to operate safely, sustainably and profitably, particularly in the offshore environment, through liaison with national, state and territory governments.51

Australian Marine Oil Spill Centre

The Australian Marine Oil Spill Centre (AMOSC) was established by the oil and gas industry in 1991 to address the issue of oil spill response within Australian waters. The centre is financed by nine oil companies and other subscriber companies. Together, these companies carry out the vast majority of the oil and gas production, offshore pipeline, terminal operations and tanker movements around the Australian coast.

AMOSC aims to provide rapid response to a major oil spill anywhere around the Australian coast. The centre manages Australia’s stockpile of major oil spill response equipment on a 24-hour stand-by basis from Geelong, Victoria. This location places the response centre at the heart of oil movements in Australian coastal waters and means it is serviced by good road and air transport access.

The centre includes a training facility for industry and government personnel, with training courses on theoretical, planning and practical issues of oil spill management—including oil spill awareness, response operations, management and command and control functions. The courses also include competence-based assessment in line with the Australian Quality Training Framework (AQTF).

The AMOSC resources, equipment and services are available to all interested parties and there is also a plan (AMOS Plan) under which company-owned equipment is shared under a voluntary mutual aid arrangement provided under the umbrella of the AMOSC hiring arrangements. The AMOS Plan is managed by AMSA on behalf of the federal, state and Northern Territory authorities and the oil and shipping industries. The oil industry contributes to the equipment and running costs of the Plan through the federal levy on shipping.

AMOSC also undertakes inspections and reviews of oil spill response plans and operations for oil companies, and can take on a quality-assurance role with members on request.

In addition, AMOSC is one of eight members of the Global Response Network (GRN), a coalition of major oil spill response companies throughout the world that distributes spill response knowledge and expertise among its members. Through this coalition individual members also have the option to develop bi-lateral agreements with other members to share resources during a spill.52
Inquiry observations, recommendations and options for Australia

During the course of the Inquiry a number of areas of primary concern or interest were identified which, while not discrete, will be important to consider when assessing the quality and effectiveness of current security arrangements. The identified areas are:

- security preparedness;
- on-site security audits and inspections;
- active on-site exercises;
- access and egress security;
- security exclusion zones;
- government and industry interaction and relationships;
- incident response – capacity, command and control;
- recruitment and vetting;
- training and awareness; and
- cyber security.

These issues are specifically considered in the assessment of the Australian oil and gas environment.

Introductory comments

The oil and gas industry operating in Australian waters has well-developed and tested safety and environmental response arrangements and a culture of safety that is, understandably, more fully developed than that of security. Although companies are continually improving their security arrangements and practices, the standard of security awareness and preparedness across oil and gas operations is currently variable.

Major international companies are likely to have well-developed preventive security regimes in place. For example, they may undertake risk assessments of all their operations, assigning them a risk category with specific security requirements and standards that must be met in addition to local government requirements.

Companies with less international experience or smaller-scale operations, may have less rigorous and comprehensive security programs and face more difficulties in implementing a comprehensive security regime. However, the Inquiry observed several examples where industry has demonstrated a willingness and ability to address security gaps and weaknesses, even when under no regulatory pressure to do so.

In terms of incident response capability, most companies maintain crisis management centres and have well-practised procedures, drills and exercises. While these arrangements and activities are primarily focussed on safety related issues and responses, there is an obvious overlap and interaction between safety and security, and the benefits of practice and exercises potentially flow to both safety and security.

The security risk factors identified by offshore operators include extremist groups (mainly environmental), criminal activity, cyber security and access control from both sea and air. Industry recognises that, while the likelihood of a deliberate terrorist-style incursion or attack within Australian waters is generally recognised as low, the risk of such an incident cannot, and should not, be disregarded. If a serious, deliberate incident was to occur the consequences could be potentially devastating in terms of safety of personnel, and economic, environmental and political consequences.
However, most offshore facilities have, in addition to manual shut-off switches, automated systems that stop the flow of oil or gas in case of an unusual event. If a system or structural failure would occur, or if a security event would cause this failure, the safety valves will shut off the flow of oil or gas on wellheads when sensors detect a drop in pressure at the surface. In such an event, the amount of oil or gas that would be released would be limited to the amount of oil or gas present in the flowlines from the sea floor to the facility.\footnote{53}

Some operators involved in joint venture or multi-facility operations require detailed risk analysis of each other’s security plans and develop a bridging plan to ensure all parties are working towards a common security standard. The bridging plan is a dynamic document which is regularly reviewed to ensure its currency. Other companies issue a Declaration Of Security (DOS), as required by MTOFSA, between the facility and a support vessel or a supply and transit helicopter.

Most offshore operations have incident or crisis management centres with well-established and practiced communication arrangements, control protocols offshore and onshore.

Facility emergency-response operation centres visited by the Inquiry were found to be well equipped with phones, radios, tabards; whiteboards, site maps and plans, procedure manuals, scenario boards, risk mapping boards and head count boards. They also have monitoring systems for CCTV, TV, wind speed and direction, and process control.

The emergency-response operation centres are usually duplicated in the head office of the company. Both centres operate together on any safety or security situation. The offshore facilities visited also had an emergency response annexe or space within the control room dedicated to the control and communication functions of incident management, including communication with local and head-office emergency management centres.

However, offshore facilities have limited resources for routine monitoring and surveillance of the facility and adjacent waters. Visual detection of small craft is limited by the number of employees working on the decks and to daylight hours, as most small craft are not lit at night.

Additionally, the degree to which companies induct or involve the general workforce operating on facilities in security preparedness and planning arrangements is significantly variable. In some cases the plans are not made available to the crews working and living on the facilities and employees are not briefed as to actions to be taken if the facility is threatened, under attack or if a hostage situation develops. On a number of facilities, the only person onboard who demonstrated a working knowledge of the security plan was the facility manager.

There are significant historical data to suggest that, even when frequently reviewed, threat assessments may not identify new or emerging threats. In particular, these include threats posed by disgruntled or trusted insiders, extreme activists and cyber intruders. Such events, as has been demonstrated by events in many parts of the world, may not be preceded by any specific intelligence or information.

As a consequence, an effective security management framework within the oil and gas resources sector is only likely to be achieved and maintained, in the opinion of the Inquiry, if there is a recognition that threats potentially exist at every facility.

The following issues are those identified during the inquiry process as areas of particular vulnerability that warrant consideration with a view to change and improvement.
Security oversight

Within the Australian context, much of the current and proposed infrastructure is in northern Western Australian waters, where the population is small and access to government resources such as the police, BPC and other services is limited. This has some obvious implications for safety and security, particularly with regard to response times and capacity in the event of an emergency, especially in OCS waters.

In overseeing or regulating the oil and gas industry, the major countries have essentially adopted two different approaches: either a prescriptive regulatory approach or a safety-case based self-regulatory approach. Both systems offer benefits and disadvantages.

Within the US an essentially prescriptive regulatory regime is in operation with the nature and scope of regulation being subject to further review and analysis as a consequence of the ‘Macondo’ Deepwater Horizon incident on 20 April 2010. However, in discussions with the inquiry team, indications were given that the US may move to a hybrid safety-case approach under which certain aspects of the current prescriptive regulations may be relaxed.

The US security threshold for regulatory oversight is governed by the United States Maritime Transportation and Security Act (MTSA) and is set according to production or personnel thresholds. If a facility produces more than 100,000 barrels of oil per day or 200 million cubic feet of natural gas per day, or hosts more than 150 persons on the facility for 12 hours or more in each 24-hour period continuously over 30 days or more it will be subject to security regulation. There are some concerns over these thresholds, however, and it is understood they are being assessed with a view to increasing the number of facilities subject to security regulatory oversight.

The Deepwater Horizon incident demonstrated the risks of having arbitrary threshold levels and boundaries for security regulation. The Deepwater Horizon facility, as a drilling unit rather than a production facility, did not meet the criteria to be subject to security regulation. Even during drilling operations such units are at risk of an incident, including deliberate attack, that could have significant consequences.

New regulations, introduced within the US, as a consequence of Deepwater Horizon are intended to further identify ‘all-hazards’ protections and requirements with modelling and risk assessments conducted and exercised against an ‘all-hazards’ framework to establish appropriate risk-mitigation strategies.

In the UK, following the explosion and fire on the Piper Alpha platform in July 1988 in which 167 people died, the Cullen Inquiry made 106 recommendations for improving control of major hazards offshore, all of which were accepted by government.

The pre-existing suite of regulations (so-called prescriptive regulations because they set specific requirements on duty holders) were replaced by goal-setting regulations.

The corner stone of the current UK regime is the creation of a safety case for each installation that demonstrates how a facility will respond and manage a major accident or hazard. The UK HSE must accept the safety case before the facility can operate on the UK Continental Shelf. While the safety case approach focuses on safety and environmental risk, the requirement to assess all potential risks includes security as a core element within the safety case regime.

Similarly, Norway has moved from a system of strict regulation and inspections by the Norwegian Government to a system of self-regulation that makes industry responsible for the safety and security of everyday operations and the implementation and management of crisis management systems.
Companies operating within Norwegian waters must be able to show clear evidence during the application stage for an operational license of how they will safely and securely manage their systems and operations for oil or gas production.

These competing international approaches to oversight and governance are further assessed in this report.

In any major safety or security incident the first response of the offshore industry will, in almost all circumstances, be to shutdown the facility and evacuate all personnel. Industry will then initiate either individual or collective corporate action to counter any human or environmental damage or danger that may result from an incident (such as a gas explosion or an oil spill). These actions, however, may not be possible in response to a deliberate attack upon a facility where, for example, hostages have been taken and/or armed intruders have taken control of the facility.

Many of the issues that may arise from a deliberate security breach or incident involving violence may be beyond the role and capacity of industry and may be matters for which government will need to assume responsibility.

While there may be a strong argument that responsibility for security prevention is largely the cost of doing business and should rest with industry, international experience indicates that the issues and challenges likely to arise from a security incident are much more likely to cause the accountability for response to lay with government.

However, during the course of the Inquiry it became apparent that the criteria within Australia governing the industry and government interface in a security incident situation is not well understood. Arrangements are unclear and in a range of potential situations, other than an unambiguous counter-terrorist attack governed by the national counter-terrorism plan, there is no common understanding of where responsibilities and accountabilities currently rest.

Under Australia’s federal governance procedures, there are complex jurisdictional issues governing regulation of the offshore industry. Under current arrangements, companies have to comply with federal, state and territory legislation as well as international law. In the case of a serious incident, the overlap of these laws and the multiplicity of agencies with varying and, on occasions, overlapping responsibilities, have the potential to create uncertainty, confusion and delay if not well understood.

The JPDA is an area of particular sensitivity. It is governed by the 2002 Timor Sea Treaty between the government of East Timor and the government of Australia (Timor Sea Treaty) and by the Treaty on Certain Maritime Arrangements in the Timor Sea (CMATS Treaty). Under the latter, Australia and Timor Leste, as signatories, may make arrangements for responding to security incidents within the JPDA. It is understood however, that these arrangements have yet to be clarified and agreed.

Apart from maritime security of loading jetties, which is regulated under MTOFSA, onshore oil and gas infrastructure, including facilities designated as critical infrastructure, is not subject to security regulation and there is no direction from government as to how such facilities should be secured.

**Security preparedness**

Security of the Australian offshore oil and gas industry is regulated under MTOFSA with the main aim of MTOFSA regulation being to safeguard the industry from terrorist attack or criminal interference.
As part of these regulatory arrangements, all offshore production facilities operating within Australia’s EEZ are required to have in place Offshore Facility Security Plans. These security plans contain a range of compliance and reporting obligations and are subject to approval by the Secretary of the Department of Infrastructure and Transport.

Originally, transport related security was regulated by the *Maritime Transport Security Act 2003* (MTSA), which gave effect to Australia’s international obligations under the ISPS Code. This code however, did not mandate security regulation to offshore oil and gas facilities.

Following the findings of the Tonkin Report, the MTSA was amended to include direct reference to offshore oil and gas facilities and was renamed the *Maritime Transport Offshore Facilities Security Act 2004* (MTOFSA). The Act is regulated by OTS, which, in accordance with current government policy, applies a risk-based intelligence-led approach to its regulatory role and functions.

Under the current statutory arrangements, only those facilities engaged in production activity and FPSO and FSOs that can operate as facilities, are subject to regulation and required to have a security plan.

Facilities involved in exploration, construction, pre-production or other preparatory activities do not fall under the MTOFSA requirements, even if in close proximity to regulated offshore production facilities.

Under its regulatory umbrella it is understood that OTS currently holds about 30 offshore security plans, covering the operations of 72 offshore production facilities and some 13 service providers, operating within the Australian 200 nautical mile EEZ. Fourteen individual companies are believed to be responsible for the operation of these facilities.

On the basis of the current risk-context approach, facility security plans are only subject to desktop assessment and review, and few physical on-site security inspections are currently conducted. It is understood that, since security regulation of the offshore environment commenced in 2006, desktop security audits of only eight offshore production facilities and one on-site security inspection (conducted in 2007) have been undertaken. All operators met ‘full compliance’ standards with respect to the desktop audits.

Actual on-site inspections of offshore oil and gas facilities are costly and resource intensive. Facilities can, generally only be reached by helicopter flights over open water, and inspectors must undertake extensive survivor safety training before travelling offshore by helicopter.

OTS advised that inspections of onshore supply base providers (vessel and aircraft operations that service offshore facilities) occurred during 2009 and 2010, although none were conducted during 2011 due to the low-risk rating and competing priorities.

ASIO’s Threat Assessments and the Offshore Oil and Gas Security Risk Context Statement, have however, reaffirmed that critical infrastructure in the energy sector, including offshore facilities, is potentially attractive as a terrorist target.

Additionally since 2008, whole-of-government reviews of civil maritime security arrangements have identified the strategic and economic importance of Australia’s offshore sector and have recommended measures to enhance collaborative security efforts in this area.
Several other factors combine to suggest that a review of the current security regulation of the offshore oil and gas sector may be warranted. These factors include: the growth in the offshore oil and gas infrastructure in Australian waters, the economic and political importance of the oil and gas industry to Australia’s future, the increasing significance of the Indian Ocean and the wider Asia Pacific region and the criticality of ensuring energy supply lines.

Expanding the range and scope of security regulation to match that of the safety regime would afford protection to pipelines, offshore exploration, drilling and construction infrastructure, and onshore facilities such as processing plants and storage areas located adjacent to security regulated port facilities.

Globally, the oil and gas industry see pipelines as the soft underbelly of the security regime and recognise that their ability to protect pipelines is severely limited due to the resources and technology that would be required. Normally, pipelines are laid directly on the seabed in deep water and are buried or covered in some form for protection in shallow water, such as harbour approaches, port areas and in areas where pipelines extend from the sea onto the shoreline at production sites.

Extending the onshore regulatory security umbrella to match that governing safety, would provide a consistent regulated safety and security environment across the Australian oil and gas industry spectrum.

Any proposed enhancements to the MTOFSA could also be supported by a criticality assessment and/or vulnerability assessment, as previously conducted by ASIO for other sectors and critical infrastructure.

**On-site security audits and inspections**

As evidenced by the practices in the US, UK and Norway, active audits and inspections are recognised as a vital part of the compliance framework in the offshore environment.

Within the US environment annual examinations are conducted on both crewed and remotely operated offshore facilities and drilling rigs, with the inspections covering the implementation and maintenance of both safety and security standards and preparedness. Similarly, in both the UK and Norway ‘all-hazards’ audits are also conducted.

In the UK, the HSE inspects all offshore installations annually on a fee-for-inspection basis with audits ordinarily lasting for a minimum of two days. A similar approach is adopted by the PSA in regard to audits in the Norwegian offshore facilities. While the focus of both audit processes is on safety, they are intended to address all relevant hazards associated with facility operations.

The Macondo incident in the Gulf of Mexico highlighted the importance of an effective audit regime and the Montara incident in Australia’s north-western waters, led to a recognition of the benefits that would flow from a seamless, national approach to safety and environmental regulation of the offshore industry.

In the opinion of the Inquiry, the current Australian situation is unsatisfactory and arrangements should be implemented that provide the capacity for an effective offshore security audit program to be introduced and maintained.

An effective audit security program will enable a much more accurate assessment to be made of the current state of facility security preparedness and will facilitate the identification of gaps and weaknesses in the operational arrangements.
As an outcome of the Montara Commission of Inquiry report and the Productivity Commission Report of 2009, the role of NOPSA has recently been expanded to include environmental protection and the authority was renamed as the National Offshore Petroleum Safety Environmental Management Authority (NOPSEMA).

The NOPSEMA safety-case approach to its regulatory role covers all offshore facility operations and is not limited to the regulation of production facilities as is OTS under the MTOFSA provisions.

It is understood NOPSEMA currently oversight some 200 offshore facilities and conduct about 160 safety audits per annum.

However, the current approach to overseeing operational risks in the oil and gas industry is siloed and divided, with different agencies having responsibility for different risks and hazards.

At present, industry operators develop measures that must satisfy two distinct regulatory regimes, provide safety cases and offshore security plans to different agencies, and ensure compliance with different and potentially conflicting legislative requirements.

While safety and security requirements are different, there are large areas of overlap, interaction and even tension that may benefit from a more cohesive safety and security audit approach.

Providing a single agency with the authority to conduct combined safety and security audits under the umbrella of an holistic ‘all-hazards’ approach to the maintenance of a safe and secure operational environment may lead to higher levels of preparedness and protection.

Whether a decision is taken to continue the separation between safety and security audits and inspections or to require a single agency to undertake both safety and security audit activities, the agency given the responsibility to conduct security audits must be sufficiently resourced to do so to a level that ensures adequate effectiveness and compliance.

Options for consideration include the transfer of security regulation of the offshore oil and gas sector to NOPSEMA, with a widened remit to combine safety and security functions; to adequately resource OTS to carry out these responsibilities, or to transfer the security responsibility to BPC, AMSA or another law enforcement agency with capacity, or ability to acquire capacity, to perform the function.
1. RECOMMENDATION

The Inquiry recommends that the Australian Government enhance the current security compliance arrangements by implementing a formal offshore oil and gas production facility on-site audit and inspection program sufficient to confirm the quality and adequacy of security measures and the levels of understanding required by an offshore facility security plan.

POSSIBLE OPTIONS:

1.1 Provide a single agency with the authority to conduct combined safety and security audits under the umbrella of an holistic ‘all-hazards’ approach to the maintenance of a safe and secure operational environment and adequately resourced to effectively perform the combined role.

1.2 Retain the current separation between safety and security audits and inspections, and equip the agency given the responsibility for security audits with the resources necessary to effectively perform the role. Approaches could include:

   – increasing the resourcing and capacity of the Australian Government’s Office of Transport Security (OTS) to enable them to conduct effective offshore security audits and inspections; or

   – transferring the security responsibility to the Border Protection Command (BPC), the Australian Maritime Safety Authority (AMSA) or another law enforcement agency with the capacity, or ability to acquire capacity, to conduct on-site compliance security inspections of offshore oil and gas facilities.

1.3 Require contract and subcontract companies to operate in accordance with the security plan of the principal operator or contractor. This will strengthen offshore security of contract and subcontract arrangements.

1.4 Amend the offshore and onshore regulatory framework by expanding the range and scope of security regulation to match that of the safety regime. This will afford protection to pipelines, offshore exploration, drilling and construction infrastructure and onshore facilities (such as processing plants and storage areas, located adjacent to security regulated port facilities) to achieve ‘whole-of-industry’ security consistency.

Active on-site exercises

In Victoria, the offshore industry operating in the Bass Strait and at the Longford Gas Plant exercise with Victoria Police on a regular basis. Within the Western Australian environment, Western Australia Police undertake a similar exercise program and there are regular water police and tactical response group deployments on near-shore and offshore facilities. It is understood, however, that there have been no recent exercises involving federal departments or agencies on offshore facilities in the NWS area or in Bass Strait.
In the UK North Sea offshore zone, the Grampian Police undertake major multi-day exercises that include all safety and security plan issues. During these exercises, the offshore industry assesses both their individual and industry’s overall capacity to respond effectively to a safety and/or security situation. Similar regular security-related exercising with offshore facilities is undertaken in the North Sea by Norwegian defence and police forces and within the US offshore environment by the USCG, FBI and defence. In each of these countries, active exercising on selected offshore facilities is recognised as an important part of the incident preparedness and prevention process.

In the opinion of the Inquiry, similar programs should be initiated in the Australian environment.

The ADF has independently recognised the importance of offshore security exercises and it is understood discussions have already commenced between the ADF and industry with a view to the early commencement of an active offshore facility security exercise program.

The ADF has also indicated an intention to appoint a senior defence person as an industry liaison officer in the NWS and Timor regions and has emphasised the importance of direct liaison between defence and industry as a key part of the security framework. The ADF also expressed interest in embedding defence force personnel on offshore facilities for familiarisation and assimilation purposes and identified to the Inquiry the importance of such deployments to the overall issue of response preparedness.

Industry has expressed a willingness to assist government agencies in developing an improved understanding of offshore facility operations and security by facilitating on-site visitations, short term familiarisation tours and deployments. They have also expressed willingness to participate in offshore facility security exercises with the ADF and with state and territory police forces. State police, who currently engage in some deployment activity on offshore facilities, and the ADF and BPC, have supported this initiative.

The benefits of short-term deployments and exercises are mutual. Industry will gain an improved understanding of the capacity and ability of government agencies to support and respond to any issue or incident offshore, and ADF, BPC and police personnel will improve their understanding of the offshore facility environment within which they may need to operate.
2. **RECOMMENDATION**

The Inquiry recommends that the Australian Government and relevant state and territory governments agree to establish an active, ongoing exercise program for selected offshore oil and gas facilities, sufficient to ensure that relevant government agencies are adequately informed, practiced and prepared to mitigate or respond to a serious offshore security incident.

**POSSIBLE OPTIONS:**

2.1 Establish a program of periodically active Australian Defence Force (ADF) and combined ADF/BPC/police exercising on, and in the vicinity of, major offshore oil and gas facilities.

2.2 Obtain agreement with industry for ADF and BPC personnel, police and other relevant agency representatives to participate in periodic familiarisation tours and deployments to selected offshore facilities—this will improve their levels of knowledge and understanding of facility infrastructure and operations and their overall level of incident preparedness.

2.3 Include sufficient government agency and private operator engagement in company and facility security planning and active on-site exercising—this will ensure that government emergency response personnel gain an accurate and realistic understanding of the knowledge, technical expertise, response and recovery skills of facility operators and other industry experts.

**Access and egress security**

There are wide variations in the access and egress security of onshore facilities, including maritime ports, heliports, LNG plants and other facilities related to the oil and gas industry. These variations include selective, or incomplete, photographic identification of passengers; a lack of segregation between passengers and other people accessing the facilities; partial screening, or no screening at all, of baggage, stores and equipment; no screening of vehicles; and incomplete surveillance of site boundaries and entry points.

These variations are not in breach of current regulations or requirements and the security standards are set by the company or operator according to their assessment of the risks. The variations, however, create points of vulnerability that should be addressed to achieve more consistent and effective security standards and arrangements.

The quality and effectiveness of onshore heliport or maritime departure points for offshore facilities are important to the maintenance of offshore safety and to minimising the risk of deliberate security incidents. The integrity of this regime assumes increased significance when linked to the unavoidable limitations in vetting arrangements for employee recruitment and the changing nature of the employee profile. Access controls for port and landside facilities are similarly variable and were found to frequently demonstrate areas of vulnerability, particularly with regard to the ease of unauthorised access.
Arrangements for the security of Australian onshore infrastructure are predominantly managed by contractors who supply security staff trained to minimal Certificate II or III standard. The Inquiry team’s observations indicate that many of these staff may not be proficient in the monitoring and screening of persons and vehicles or be trained to an acceptable standard on the operation of relevant screening equipment. Similarly, the quality of the supply-chain and supply-base security arrangements for these offshore facilities is an issue of concern.

Currently, a supply base is determined to be a place where passengers and/or goods are finally loaded for transport to an offshore facility. Although these transport providers are subject to MTOFSA security regulations as service providers, the requirements of the regulation are minimal. There is no requirement to undertake specific screening of either passengers or goods. Additionally, a land-locked logistics base or a service provider, such as a food provisioning company that packs goods into sealed containers for transport to heliports or maritime ports for offshore delivery, are not subject to any security regulation.

**Heliports**

Heliports servicing the offshore oil and gas industry have a variety of security arrangements in place to meet government regulation and operator requirements. Heliports located within Aviation Transport Security Act 2004 (ATSA) regulated airports usually operate from separate general aviation aircraft aprons to RPT aircraft and are, as a consequence, not subject to any regulatory aviation screening of passengers, baggage and stores carried by helicopters. Offshore helicopter operations, considered to be operating as service providers under MTOFSA, are required to have an approved maritime or offshore facility service-provider security plan. On the other hand, private airports that are not subject to ATSA security regulation and who operate in support of offshore operations are required to have a MTOFSA port-facility security plan.

While the number of heliports currently servicing offshore infrastructure within the Australian EEZ is low (currently assessed at less than 10), the current variations in security screening practices should be addressed and will benefit from review and regularisation.

The cross-jurisdictional nature of the requirements for offshore security plans for helicopter and supporting airports exists due to the absence of specific security arrangements under ATSA for non-RPT aircraft. Helicopter operations from regulated airports are subject, however, to the general provisions, including access controls, of the ATSA-regulated airport security plan.

In some cases, the seaport or offshore facility associated with the airport or heliport is hundreds of kilometres away, including in another state or territory, and yet required, under MTOFSA, to provide a port security risk assessment to assist the airport or heliport in developing its own maritime or offshore facility security plan. It is doubtful if such arrangements are appropriate for developing an effective airport or heliport security plan in these distant locations.

Airports and heliports with a MTOFSA port facility, port service provider or offshore facility service provider security plan were found to have staff who did not display the MSIC as a means of access control or identity. Essentially, airlines and helicopter operators contracted to offshore operators provide the level of security and safety detailed under their contract. If specific security requirements, such as screening of personnel, baggage and freight are not included in the contract, then these services are not provided. Similarly, as mentioned earlier, where offshore operators provide their own security regime, the requirements can vary from full screening of passengers, baggage and freight to minimal identity checking.
Some companies have voluntarily adopted best-practice security screening that is equivalent to ATSA-regulated RPT security screening requirements and includes screening of passengers, baggage and freight. This is consistent with practices observed by the inquiry team in the US during its international assessments. However, in some cases different operators are employing fundamentally different levels of security checking and screening within the same regulated airport boundary.

Some offshore facility helipads observed by the Inquiry team, both in Australia and the US, were undertaking the double-checking of bags on arrival and exit from the offshore facility, and there were several instances where handheld metal detectors were available for random screening for both arrival and exit. This is, however, not currently standard industry practice within Australia.

A number of approaches could be considered to improve the consistency and quality of access security to offshore infrastructure. These include adoption of RPT security standards and screening arrangements currently in place at regulated Australian airports or by voluntarily settling minimum access security standards, agreed as appropriate for heliports and maritime ports which service offshore facilities.

**Supply and support vessels**

Maritime ports that service shipping regulated under ISPS Code provisions are regulated under MTOFSA. However, ports that service offshore support vessels of less than 500 gross register tonnage are not included under the MTOFSA provisions and, consequently, are not subject to regulation. This presents as a potential security risk to offshore facilities and operations.

The continued growth of the Western Australia offshore oil and gas industry will see current operations expand and the introduction of new operators. Industry expressed concern at the lack of skilled and qualified Australian seafarers available to crew the additional vessels needed to support such expansion. To meet this demand, foreign ships and foreign crews are being increasingly introduced into the Australian offshore maritime industry.

Ports Australia raised this issue as a particular concern, especially with regard to supply vessels operating in the NWS, and the increasing use of vessels of doubtful suitability and questionable crew competencies across a range of offshore operations.

There are several other areas of concern that warrant further examination. For example, some Australian-regulated vessels may have foreign workers as part of their crew complement under 457 visa arrangements; foreign registered vessels may have Australian or foreign crew; and the fact that foreign-registered vessels are security-regulated under the ISPS Code security provisions of the flag state rather than under MTOFSA. In the latter case, ISPS Code provisions may differ from the requirements of MTOFSA and the crews may or may not have security checking standards equivalent to MSIC. In addition, some foreign-registered vessels will use overseas ports or heliports for crew transfers and this means that there will be no security check by Australian Government immigration and customs agencies, as would occur when a foreign registered vessel undertakes a crew change through an Australian port.
3. **RECOMMENDATION**

The Inquiry recommends that agreement is reached between the Australian Government and industry on identifying consistent minimum standards of security and screening arrangements for all offshore access and service-delivery aviation and maritime ports.

**POSSIBLE OPTIONS**

3.1 Implement airport Regular Passenger Transport (RPT) security standards and screening arrangements, currently in place in regulated Australian airports, at onshore heliports servicing offshore oil and gas facilities.

3.2 Extend the security provisions of the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) security to cover all currently unregulated maritime ports and facilities that operate as a supply point to service offshore oil and gas facilities.

3.3 Hold consultations between the Australian Government and industry to reach agreement on the minimum security standards for access security at all heliports and maritime ports servicing offshore facilities, with such standards to be settled and observed by memorandum of understanding (MOU) or regulation.

**Security exclusion zones**

The original internationally agreed 500 metre safety exclusion zone was established under Article 60.5 of UNCLOS in 1982. The article stated that a state may establish reasonable safety zones, not in excess of 500 metres, around their offshore facilities. Within the Australian environment, a similar 500-metre security zone has since been established under MTOFSA.

The current internationally agreed 500 metre offshore security exclusion zone arrangement available to oil and gas facility operators is commonly agreed as too small and not offering adequate protection to operators.

While 500 metres is also the safety-zone limit, the safety-zone boundaries cover all offshore facilities, including wellheads, linked pipelines and hubs as identified by the facility operator, under their safety plan with NOPSEMA. This wider boundary applies despite the fact that a safety zone is only intended to protect the facility from unintentional incidents or emergencies.
The maritime chart extract of chart Aus357 in Bass Strait, developed for the Inquiry by the RAN Australian Hydrographic Service, shows the current 500 metre MTOFSA Security Zone in place around offshore production facilities in Red and the NOPSEMA Safety Zone shaded in Pink. Note the difference in size/area of the safety zone encompassing the facilities, undersea well heads and connecting flow-lines to the security zones currently in place around the individual offshore production facilities. The Exclusion (Orange) and Area to be Avoided (Blue) Zones proposed under Option 4.1 are included for comparative purposes.
Within Australian waters, the security zone is available to oil and gas facility operators under MTOFSA, who may request the Secretary of the Department of Infrastructure and Transport to declare an offshore waterside zone around a security-regulated offshore facility. Details of these zones must then be included in the maritime security plan of the relevant facility. In particular, the operator must identify the boundaries of the zone; the security measures, that will be taken to control access; and the steps to be taken to inform people of the existence and boundaries of the zone and that entry into a zone, without authorisation, is an offence.

The current determination of 500 metres as the maximum distance at which a security zone can be declared, however, makes the zone largely ineffective. The zone is difficult to demarcate and allows vessels to approach too close to an operating facility before any preventive action can be taken, particularly if there is any malicious intent on the part of the intruding vessel. In addition, breaches of the 500-metre zone are largely unenforceable and current reporting arrangements largely, ineffective.

There is an argument that facility operators, who have ultimate responsibility for the safety of crew on a facility, require sufficient time to assess and respond to a possible security threat in an effective way, and to minimise any risk presented by the threat.

A large, fixed production platform will take about 30 minutes to evacuate once a general alarm is sounded. However, in that time, a vessel travelling at 20 knots will travel about 10 nautical miles. This distance equates to the normal range of visibility between a facility and the horizon. Operators and crew also provided numerous examples to the Inquiry of incidents involving fishing and recreational craft operating in close proximity to a facility and ignoring the 500-metre exclusion zone, including instances where there were attempts to moor alongside or board the facility.

Offshore facilities, especially those closer inshore on the NWS, have had a number of small recreational and commercial fisherman incursions into the exclusion zones, in particular off Varanus Island, Barrow Island and the Wandoo platform. Vermilion Oil’s Wandoo B platform is close to Dampier and is regularly visited by local recreational fisherman due to the congregation of fish around the platform. Small craft have moored to the platform and CALM buoy and requested assistance when weather conditions deteriorate. An Inquiry team visit to an FPSO in Australian EEZ waters off Western Australia witnessed the close approach of small foreign fishing vessels to within 30 metres of the FPSO facility. The FPSO had no method of enforcing or controlling access into the 500 metre safety and security exclusion zones in place around the FPSO.

Offshore facilities have difficulty in determining the identity of a vessel and its intent when it approaches without appropriate authorisation. Although some offshore facilities maintain a larger safety and security exclusion zone than the 500 metres stipulated by the UNCLOS Convention and IMO Guidelines, these enlarged exclusion zones have no legal weight and the only action that a facility can take against an approaching vessel outside the 500-metre zone is to communicate a radio warning.
A recommendation by the IMO, Resolution A.671(16) on safety zones and safety of navigation around offshore installations and structures suggested that governments consider establishing safety zones around offshore installations and structures. In addition, the IMO recommend the establishment, and charting of, fairways or routeing systems through exploration areas. Currently the IMO can approve the following ship routeing systems: traffic separation schemes, traffic lanes, separation zones or lines, recommended routes, precautionary areas with defined limits where ships must navigate with particular caution and areas to be avoided in which either navigation is particularly hazardous or it is exceptionally important to avoid casualties and which should be avoided by all ships, or by certain classes of ships. An example of an IMO-approved area occurs in Bass Strait; it concerns an ‘area to be avoided by all ships over 200 gross registered tonnes’, which was approved in 1981. This area, which is larger than the UNCLOS 500-metre exclusion zone limit, is in place to reduce the risk of collision by large vessels with the numerous petroleum installations in Bass Strait.

SIEVS have arrived at offshore facilities in a number of areas in northern Australian waters and, while it is difficult for those onboard the SIEV to directly access a facility, their presence alongside may place ongoing oil and gas operations at risk. This situation is aggravated by industry’s concerns over the variability and uncertainty of government response to such incursions and the ability of exclusion zone incursions to be effectively enforced. This concern is to some extent corroborated by the fact that only one successful prosecution, against the captain of a commercial fishing vessel for unlawfully entering into an offshore facility exclusion zone, has occurred in Australia since regulations took effect.

Offshore companies have responded to the possible arrival at facilities of SIEVS by producing operational procedures for such an eventuality and, in some cases, by placing communication booklets—in relevant languages—on how to communicate with SIEV persons on all offshore facilities and support vessels.

The security exclusion zone concerns discussed above are currently subject to review. Industry and government are undertaking important research and development activity into their effectiveness. As part of this process, the Australian industry and government OGSF has formed a working group to examine the options for achieving offshore exclusion zone improvements. In particular, the working group will look at exclusion zones and areas to be avoided, their effectiveness and enforcement, and assess known and suspected breaches that have occurred in currently established zones.

In addition AMSA, under its ‘Safe Horizons’ project, has reviewed current exclusion zones in place around offshore facilities in north-west Australian waters. These were reviewed in the light of ongoing increases in shipping traffic and the upgrades and new developments of ports. In particular, the review—advised by extensive consultation across government and industry—focused on maritime safety and environment protection in ship routes. It assessed measures for current and future maritime activity, coastal vessel traffic management, and increased use of AIS for shipping, offshore facilities and navigation aids. The implementation of the nine recommendations from this review is currently being lead by AMSA and the Western Australian Department of Transport, as appropriate.

During roundtable discussions between the Inquiry and industry security representatives, a proposal was put to the Inquiry that consideration be given to replacing the current 500 metre security zone limit with a three-tiered boundary approach to security zoning that would apply to all offshore facilities within Australian waters.
The proposed industry model comprised:

1. a cautionary zone associated with traffic separation schemes, traffic lanes and recommended routes of 15 nautical miles from any offshore facility that requires vessel operators to make and maintain communication with facilities within its radius;

2. an area to be avoided of 5 nautical miles from any offshore facility that acts to prohibit entry into the zone by non offshore facility related shipping; and

3. an exclusion zone, within the area to be avoided, of between 1 and 2.5 nautical miles for all shipping unless directly related with the facility operations and then only with express approval to enter having been given by the operator.

It is anticipated that this proposal is likely to be subject of discussion as part of the OGSF working group discussions on this subject.

However, it will be important, in any discussions, to assess the implications that any boundary changes may cause. This includes taking into account that there are as many as seven different data sets that identify the locations of offshore facilities within the Australian EEZ. Additionally, the shipping fairways being proposed by AMSA, which chart shipping lanes, while not mandatory, will need to be taken into account in any considerations of change. Any agreement to enlarge these boundaries would also need to be discussed and settled with IMO in order to have appropriate international recognition.
4. **RECOMMENDATION**

The Inquiry recommends that immediate consideration is given to extending and hardening current security exclusion zone boundaries and arrangements to increase the safety and security of offshore facilities from unlawful or unauthorised intrusion and threat.

**POSSIBLE OPTIONS**

4.1 Introduce a new three-tiered approach to security zoning for all offshore facilities within Australian waters, including:

- a cautionary zone associated with traffic separation schemes, traffic lanes and recommended routes of 15 nautical miles from any offshore facility that requires vessel operators to make and maintain communication with facilities within its radius;

- an area to be avoided of 5 nautical miles from any offshore facility that acts to prohibit entry into the zone by shipping unrelated to the offshore facilities; and

- an exclusion zone, within the area to be avoided, of between 1 and 2.5 nautical miles for all shipping that is not directly related with the facility operations and to which access by can only be gained through express approval to enter given by the operator.

4.2 Establish ship routeing schemes, vessel traffic management schemes, traffic lanes and recommended routes and areas to be avoided around and in the vicinity of all offshore facilities to improve the stand-off safety distance for ship navigation around such offshore facilities.

4.3 Attribute liability for the cost of evacuation and any associated ‘shutdown’ costs to the owner or operator of a vessel who intrudes into an exclusion zone and (through the nature of the vessel’s activities) causes an evacuation of a facility—these costs to be met by the owner or operator of the intruding vessel unless the facility operator acted unreasonably in commencing the evacuation.
The maritime chart extract of chart Aus327 off Dampier, developed for the Inquiry by the RAN Australian Hydrographic Service, shows the current 500 metre MTOFSA Security Zone in place around offshore production facilities in Red and an example of the Exclusion (Orange), Area to be Avoided (Blue) and Cautionary (Green) Zones proposed under Option 4.1 for comparative purposes. Note the proximity of the current Shipping Fairway to the offshore facilities and the intersection of the Cautionary Zone with the Fairway.
Security surveillance

Whatever decision is made in regard to the current exclusion zone boundaries, additional protection, and safety and security related information could be obtained and made available to industry and relevant government agencies through the improved use of technology.

One of the systems currently under review by AMSA is the shore-based Vessel Traffic Services (VTS) system. The VTS system can provide a variety of information to ships, including position information about other traffic, meteorological hazard warnings, and even extensive management of traffic within a port, waterway or sea area of special interest. Ships that enter a VTS area have to report to authorities and may be tracked by the VTS by radar, AIS or other technologies. The ships entering a VTS area need to keep watch for navigational or other warnings on a specific radio frequency and may also be contacted by a VTS operator. The VTS system is internationally recognised and can interact with, and influence, the decision-making processes onboard a vessel. For example, it can serve as an alert system in cases of close quarter situations between vessels, a vessel and an offshore facility, or in cases of danger. The International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) has developed Guideline No. 1070 on the role of VTS in managing Restricted or Limited Access Areas.60

Restricted or limited access areas are intended to enhance the common protection of shipping, the environment and sea areas requiring specific protection by addressing the unique risks and vulnerabilities in these areas. Examples include offshore installations such as oil and gas exploration and production facilities, wellheads and pipeline networks.

Currently, there is no requirement for offshore facilities to fit and operate an AIS system for maritime shipping identification and location purposes. As a consequence, few offshore facilities either have radar fitted or operate modern ARPA type radars with AIS and automatic target tracking capabilities. There are obvious benefits in doing so and industry has indicated a willingness to participate in any initiative to equip facilities with ARPA radars and to share data.

An offshore facility AIS transmission could include information on exclusion zones and provide the facility with early identification of approaching maritime traffic.

Modern ARPA-equipped radar systems can automatically track vessels approaching offshore facilities and provide warnings at pre-set limits. The ARPA radar systems are also fitted with an AIS facility that displays vessel information such as, the name, unique international identification number, course and speed on the radar display. The system also has further information on the vessel, including type of ship and cargo, radio call sign and destination. With such a radar system, a facility could identify and communicate with an approaching vessel and advise them by radio call to avoid entering the security exclusion zone, should that be necessary.

Radar has the potential to allow offshore facilities to monitor their immediate surrounding sea area and track and identify approaching vessels. As an example of leading-edge practice in this area, the Bass Strait offshore facilities have two platforms fitted with ARPA radars that are linked to the Longford gas plant control room. At the control room, the radar pictures are combined and displayed on an overlay of the Electronic Chart Display and Information System (ECDIS). This information, combined with shipping AIS information, thus presents users with a complete Bass Strait shipping ‘picture’. In particular, the ECDIS system displays the information from Electronic Navigational Charts (ENC) or Digital Nautical Charts (DNC) and integrates position information from the satellite Global Positioning System (GPS) and other navigational sensors, such as radar and AIS.
The Bass Strait arrangements illustrate what could be achieved in locations with multiple offshore facilities. The radar and AIS data could be shared between facilities and onshore control rooms and combined with an ECDIS display to achieve integrated surveillance and close-approach response capability. The radar and AIS data could also be made available to BPC and AMSA, on an as-required basis, for enhanced surveillance and maritime domain awareness in offshore oil and gas fields.

17. Options for the establishment of Vessel Traffic Service (VTS) systems to protect offshore facilities:
   - Establish a VTS system to monitor and control shipping movements along the north-west Western Australia coast in coastal and EEZ waters to enhance safety and security situational awareness.
   - Use a VTS system in conjunction with any ship routeing schemes, vessel traffic management schemes, traffic lanes, recommended routes, and areas to be avoided to ensure that ships maintain adequate safety and security distances from current and projected offshore oil and gas facilities.

The Ship borne AIS, as specified by the IMO, is a ship and shore-based broadcast system, operating in the VHF maritime band. It is capable of sending and receiving ship information such as identity, position, course, speed, ship particulars and cargo information to and from other ships and offshore facilities, suitably equipped aircraft and shore facilities. When used with an appropriate graphical display, shipboard AIS enables the provision of fast, automatic and accurate information regarding risk of collision by calculating Closest Point of Approach (CPA) and Time to Closest Point of Approach (TCPA) from the positional information transmitted by target vessels. AIS also provides a means for communication from ship to ship or facility, and from ship or facility to shore. It can be used in search-and-rescue and can provide a means to transmit and display different types of information of safety and security importance—such as exclusion zones, navigation hazards, warning notices.

The use and application of CCTV cameras on offshore facilities and onshore production and support facilities is also variable. Offshore the CCTV arrangements fitted tend to be used for inward facing facility operational purposes as opposed to outward facing in a sea area surveillance security monitoring capacity. The ability for persons onboard the offshore facility to continuously monitor CCTV is understandably limited given their normal operational workload in a continuous production environment.

Onshore CCTV is used for perimeter and access control security surveillance purposes with security control points monitoring CCTV inputs. Additionally, industry has adopted new security technology to improve onshore production and export related facility site security including fibre optic cable perimeter fence tampering systems, infra red and CCTV cameras with motion detector capability and the use of Long Range Acoustic Device (LRAD) warning apparatus on an LNG loading jetty. These devices were demonstrated to good effect to the Inquiry team during site visitations.

The use of latest technology CCTV and/or Infra-red Thermal Imaging full pan and tilt cameras on offshore facilities with automatic video analytic detection capabilities placed facing outward for automatic sea area surveillance and alarm purposes could serve to improve overall area sea surveillance around an offshore facility without placing an increased workload on persons onboard.
18. Options to improve surveillance and situational awareness:

- Employ close-range high-definition radar with Automatic Radar Plotting Aid (ARPA) and Automatic Identification System (AIS) capability as a standard part of offshore facility security infrastructure - this will improve the quality of offshore surveillance and situational awareness.

- Establish an agreement between industry and government that facilitates real-time transfer of radar data to government agencies, such as BPC and AMSA. This will enhance maritime domain awareness in Australian offshore oil and gas fields.

- Develop a link to provide data feeds to BPC, AMSA and police, where relevant.

- Expand the current use of Closed Circuit Television (CCTV) or Infra-Red Thermal Imaging cameras to provide capacity to monitor the immediate sea area around each offshore facility.

- Improve shore-based maritime monitoring capability using facility-based radar, AIS, CCTV and Infra-Red inputs to improve surveillance and oil-field situational awareness.

- Use video analysis to provide an automatic surveillance capacity within the immediate sea area around a facility.

Additionally, offshore radio communications, traditionally fitted to offshore facilities, suit normal inter-facility, helicopter and emergency requirements and use commercial equipment and frequencies. Systems used include marine VHF and Global Maritime Distress and Safety System (GMDSS) transceivers and voice and data microwave links.

GMDSS is an amalgam of various individual radio systems, both terrestrial and satellite. The Inquiry found that the automatic messaging formats available with GMDSS were not being taken advantage of for sending safety and security related Digital Selective Calling (DSC) messaging automatically to company and government agencies. DSC is, basically, a paging system that is used to automate distress alerts sent over VHF, MF and HF marine radio systems. The message document will display in PDF format. DSC can be used to establish initial contact between the offshore facility and selected recipients and can act as an emergency SOS-type message call for a safety or security related incident if required.

Governments within Australia, as in other countries, are having difficulty keeping abreast with the developments in deepwater operations further from the coastline and in more remote locations. Many issues need to be evaluated and better understood to improve this situation. For example, how to effectively monitor the maritime domain further off the coast and those sea areas remote from each other; how to achieve the timely response to a security, safety or environmental incident; and how to assess the security risks associated with isolated offshore deepwater operations.
Similar requirements for evaluation and understanding apply to onshore facilities. Port facilities that interface with offshore facilities or loading jetties for the export of oil or gas products are regulated under the MTOFSA. Landside production facilities are not security regulated and are a potentially serious security weakness. State and territory governments have regulatory compliance arrangements for workplace safety and environmental requirements, but no specific site security requirements for the onshore facilities unless they are classified as critical infrastructure. Industry has identified that pipeline remote valve sites, which are critical to production operations are a significant onshore risk. Sites visited by the Inquiry were identified as having perimeter security, such as fencing, lights, sensors and alarms. However, there was no evidence of additional preventive security measures, such as vehicle-resistant crash barriers or widening of the perimeter area to enhance resistance to potential attack.

**Government and industry interaction and relationships**

In general terms, industry recognises that it enjoys a constructive relationship with the relevant Australian Government, state and territory government agencies. At a Federal level, these relationships are fostered through a range of informal and formal arrangements, including the OGSF, ESG and the Trusted Information Sharing Network (TISN). Industry and government forums such as the Pilbara Critical Infrastructure Security Collective, hosted by the Western Australia police, and the Gladstone Industry Development and Community forum are examples of this approach at the state and territory level.

An identified industry concern, particularly within the federal government environment, is that these arrangements currently rely too heavily on individual personal relationships and that, as a consequence, they are open to variability and sudden change. While the value of personal relationships and trust should not be underestimated and are an important part of any interagency relationship, the inquiry considers that there is a need to improve the clarity of industry and government interaction arrangements. This will provide more confidence that the quality of dialogue and effectiveness of response will not vary according to who answers the phone.

There is common agreement that increased engagement between industry and government security agencies, aimed at improving mutual levels of understanding of the intelligence-gathering analysis and dissemination process and the knowledge and expertise of industry in the security space, is both warranted and desirable. There is also growing recognition that more emphasis needs to be placed on the need to achieve a balance between the risks of sharing information and the consequences of failing to do so.

Offshore operators have access to their own industry intelligence, but may have little real knowledge of security in Australian maritime and adjacent international waters. Industry therefore relies on the Australian Government to provide sufficient intelligence to enable industry to effectively assess and mitigate risks. The industry position is that information or intelligence shared by government needs to be accurate, timely and delivered in a constructive manner, and that anything less creates a perception of a reluctance by government to genuinely engage. The international experience of industry suggests to them that the quality of information shared by Australian Government agencies is not as useful and valuable as that shared in some other countries.

These concerns suggest that within Australia, current information sharing practices and procedures between government and industry may be less than optimal. Whatever the reality, current perceptions have clearly led to a lack of confidence by industry in the quality of the product being shared. As a balance to these criticisms, however, it is clear to industry that the ASIO BLU publications are addressing some of these issues. Industry acknowledges that these are valuable and continually improving in both quality and relevance.
During the course of the Inquiry, the Attorney-General’s Department identified the need to further enhance the exchange of information with security managers of offshore oil and gas companies about ASIO’s threat assessments and operations, and seek input from industry. ASIO, through the BLU, organised a roundtable with industry, which was held in Canberra during March 2012. The forum, which was opened by the Director-General and attended by the ASIO senior executive, demonstrated the seriousness ASIO placed on achieving and maintaining genuine engagement with the offshore industry.

Although ASIO, like all government agencies, has resource limitations and is required to respond to multiple agency and industry demands and to prioritise its work, they acknowledged the need for increased cross sectoral engagement between government and industry.

During discussions with the Inquiry, ADF representatives identified the importance of establishing a consultative industry/government forum to operate complementary to the OGSF to build a stronger and more cooperative approach to security in Australia’s north west. It was suggested that an MOU between the ADF, government and industry on north west security issues may be beneficial.

A particular concern raised by industry during the Inquiry process was that they were not receiving notification from government agencies when potentially dangerous vessels entered restricted zones or were passing close to offshore facilities, despite the potential threat such vessels may pose.

Industry provided a number of examples, including one where a large private vessel, which was allegedly a vessel of interest to Australia’s law enforcement agencies, was allowed to transit through the IMO approved Bass Strait ‘Area to be Avoided’ zone. According to industry, offshore operators were not advised of the presence or passage of the vessel, or of the potential security risk the vessel’s presence created, until after the vessel had been arrested at a port some days later. Considering the number of people engaged on facilities near the area of the vessel’s transit, industry saw the lack of notification of the ship’s passage as a breach of sensible safety practices and a demonstration of a lack of trust.

While the importance of maintaining high levels of security during serious law enforcement investigations is well understood, there may be benefit in reviewing recent incidents. Such a review could be used as a means to agree on more transparent and unambiguous arrangements that more effectively balance the competing issues of law enforcement security and offshore facility safety and security.
5. RECOMMENDATION

The Inquiry recommends that active and constructive steps are taken to further improve the quality and mutual value of engagement and interaction between government and industry.

POSSIBLE OPTIONS

5.1 Increase industry and government engagement to improve mutual levels of understanding of the intelligence gathering, analysis and dissemination process, and the knowledge and technical expertise of industry with regard to security-related issues.

5.2 Change the current security clearance procedures to improve the access for designated industry security personnel to important threat information via a clear and transparent process that is demonstrably inclusive and equitable to industry.

5.3 Establish an MOU between the Australian Government and industry to underpin a new consultative forum, involving ADF representation, that meets regularly with industry representatives to address security-related issues and concerns, particularly in the north and north-west of Australia.

5.4 Strengthen the current whole-of-government approach to security in the north and north-west of Australia by widening the role and purpose of forums, such as the Oil and Gas Security Forum (OGSF), to include periodic engagement and interaction between the oil and gas industry, the maritime industry, the onshore mining industry and state and territory government agencies.

5.5 Review and assess the level of risk-sharing of normally restricted intelligence information with relevant industry stakeholders and weigh this against the potential consequences of not doing so.

Incident response – capacity, command and control

*Reporting and response capacity*

The Australian oil and gas industry is risk averse and individual corporations have put in place well developed preventative safety and security response arrangements. However, industry response to a deliberate external attack upon, or sabotage of, a facility is likely to be limited to shutting down, evacuating the facility and, to the extent possible in the prevailing circumstances, limiting damage and environmental fall out.

The attitude of industry is that dealing with the response to a deliberate terrorist or criminal act is primarily the responsibility of government. In this regard they have expressed concern and uncertainty about the ability of government agencies to respond effectively to such an incident, especially considering the remoteness of many of the offshore facilities and the competing priorities of government response agencies across the maritime domain.
The strong consensus industry view is that, apart from possible environmental and damage mitigation and some transport support activities, the response to a terrorist or serious criminal act is likely to be beyond industry’s resource capacity and will be a matter for government.

Currently, no state police force maintains a dedicated response unit for offshore oil and gas facilities and police support to offshore oil and gas has to be considered against other competing operational priorities at the time.

Companies operating in Western Australia and Victoria have developed contingency plans on the basis that the relevant state police will be the first responders to any offshore security related incident. In both states government agencies, particularly the police, are actively engaged with the offshore oil and gas industry in preparation for such an eventuality. They have assets available for deployment and are well practiced and exercised to work with industry, although their response and resource capabilities are limited, and in many situations their resources may be exhausted relatively quickly.

Though this relationship appears to meet industry expectations, it has placed a burden on local state police resources that they may not be able to meet on all occasions or in a protracted security incident situation.

In all Australian jurisdictions the difficulty of undertaking an effective police response increases the further offshore the facility is situated or the more serious the incident.

As identified in the 2005 Tonkin Report, despite the reliance placed by many companies on a police incident response, police do not have the same level of capacity to respond to an offshore incident as they do to an onshore incident. In his report, Tonkin found that continued reliance on police resources for offshore maritime security response was not a viable option and that a key policy question for government was how this capability gap should be addressed and resolved. 61

While there is a clear framework of response and accountability under the National Counter Terrorism Committee (NCTC) arrangements relating to a terrorist incident, actual agency accountability and response priorities relating to an incident for which the cause is not immediately known, or clearly not a terrorist situation, is not as well understood.

The oil and gas industry recognises that the nature and speed of government responses to a security incident will depend upon the nature and seriousness of the event and the isolation of its location. However, there appears to be need for a well-understood response framework that will engender confidence on the part of industry. Industry’s perception of the limited visibility of ADF assets and BPC surveillance and patrol activities in the NWS oil and gas fields and the absence of ADF familiarity deployments or exercises involving offshore facilities have exacerbated industry concerns.

While the ADF, particularly through BPC, has an active presence in the north and north west of Australia, activities are primarily focused on border protection with a particular emphasis on SIEV and foreign fishing vessel movements. Although these activities are consistently occurring in northern Australia waters, they are generally undertaken outside the primary oil and gas offshore fields and the presence of ADF and BPC assets is generally not known or observed by facility operators.

BPC, through AMSOC, and the Australian Maritime Information Fusion Centre (AMIFC) monitors vessel movements within the entire Australian EEZ, including detecting, tracking and threat-assessing of vessels that operate in, or approach Australia’s maritime zones. This role and function is not well understood by industry and, to the extent that it is appropriate in security terms, could be improved if more thoroughly explained in industry forums.
Another response dimension is created by the increasingly crowded and competitive services and facilities environment in the north and north west of Australia. Maritime port, heliport and airport facilities are used extensively by the oil and gas and mining resources sector and demand will continue to grow. These competing demands on transport hubs and service provider facilities may impact on the ability of government agencies, including the ADF, to effectively respond in an emergency situation.

**Command and control**

Currently, there is uncertainty surrounding command, control, coordination and jurisdiction arrangements that exist between government agencies. Legislatively, the Australian offshore oil and gas infrastructure environment is complicated by a multiplicity of federal, state and territory Acts, provisions and arrangements. This complexity has created jurisdictional uncertainty and confusion across industry and between companies and government agencies. In a number of areas, Australian and state or territory government legislation also overlaps and this may potentially delay or confuse lead agency response arrangements.

**Offshore security**

Within the Australian Government environment, BPC is officially identified as the primary government law enforcement organisation in Australia’s maritime domain. It has a lead coordination and planning role that extends to state and territory organisations. However, individual Australian Government and state and territory government agencies continue to respond and act according to their individual mandates and responsibilities. While BPC is the first point of contact for any maritime-related security-based incident, the situation may differ if the incident appears to be accidental and only involve safety issues or environmental damage, or where the cause is undetermined. In these situations the contact or lead agency, depending on known circumstances, may be either NOPSEMA, AMSA, state or federal police or industry itself.

In Western Australia, the State Department of Mines and Energy has responsibility for safety audits and inspections in coastal waters out to the three nautical mile limit. NOPSEMA has authority and responsibility for the conduct of safety audits from the three nautical mile point out to the 200 nautical mile EEZ.

Under the *Victorian Terrorism (Community Protection) Act 2003*, offshore facilities may be declared as essential services under Part 6 of the Act. However, it is understood that at the time of the Inquiry, no declaration had been made in regard to any offshore facility in Victorian waters. Under current arrangements only the Longford oil and gas plant and Long Island Refinery are identified as being of national critical infrastructure importance with only Longford having been declared as an essential service under the Act. As a consequence, the only security regime that currently covers Bass Strait offshore facilities is MTOFSA. However, the Victorian Department of Primary Industries (DPI), Security and Emergency Division, has oversight of the Longford oil and gas plant security risk management plan and undertakes annual exercises to test the adequacy of the plan. This process is supervised jointly by the Victoria Police and DPI and reported to the Minister for Primary Industries by Victoria Police as the independent assessor.
The JPDA is an area of particular jurisdictional sensitivity including doubts about incident command and control arrangements. It is governed by the Timor Sea Treaty 2002, under which Australia and Timor Leste, as signatories, may make arrangements for responding to security incidents within the JPDA. The CMATS Treaty between Australia and Timor-Leste does not deal with the issue of maritime security and jurisdiction within the JPDA sea area. While CMATS does not address security directly, it does establish a maritime commission, which includes in its functions consultation on maritime security, including the security of petroleum facilities and infrastructure. The offshore facilities within the JPDA do not need to comply with the International ISPS Code requirements for maritime and offshore facility security plans. Additionally, no offshore oil and gas facilities within the JPDA have been gazetted by the Australian government for security regulation under MTOFSA.

Oil companies operating within the JPDA can develop whatever security arrangements they deem appropriate. The current major JPDA offshore facility operator advised the inquiry that they undertake independent audits of their offshore facility security to API benchmark standards in order to have reassurance that the JPDA offshore security arrangements in place meet known standards of security compliance. It is understood that a company has moved to engage the USCG to conduct security audits on its behalf on their JPDA facilities to independently assess the effectiveness of their current arrangements.

With regard to SIEV intrusions within offshore facility exclusion zones, industry is unclear as to what their responsibilities are when those people seek assistance or when rescued persons are taken on board. Questions posed by industry include: Where should they be taken? How should they be treated? What if they have disease? How does a small crew cope with high numbers needing care and medical help? What government response could be expected? Will governments respond and remove SIEV people from the offshore facility?

The Tampa incident still colours the thinking of many in the industry and they are not confident that any positive action is being taken by government. In the Tampa incident, even though the ship’s captain acted in accordance with the SOLAS Convention, the incident created significant bad press for the shipowner. The oil and gas industry is very conscious of its reputation and is anxious to avoid risking exposing itself to adverse coverage.

The Inquiry was advised of one SIEV emergency where industry operators were in the process of organising their own medivac, medical staff and triage due to the slow response of government to the emergency incident.

Another issue that creates uncertainty over security command and control is that many facilities are run in partnerships or are part of a wider operation. Facilities run in partnership or jointly with more than one company have different levels of operational authority and roles that can create confusion. Additionally, a facility that is part of a multiple facility operation or field may be located across the boundaries of coastal and state waters and of waters within the 12 nautical mile limit or outwards towards the 200 nautical mile EEZ. Under current MTOFSA coverage, linked production facilities of a single operation run through both regulated and unregulated zones. For example, the Woodside Petroleum Rankin platform is regulated by MTOFSA, but the pipeline that runs from the facility to the shoreline is unregulated. As the pipeline enters the port precinct it enters the MTOFSA security regulated port; however, when it approaches and exits the water and enters the LNG plant it is again unregulated.
As mentioned earlier this fragmented or siloed approach to security regulation is a genuine point of security vulnerability. This vulnerability assumes particular importance when assessed against an appreciation of the interdependencies between upstream oil and gas production activities and downstream energy supply.

19. Options to strengthen Joint Petroleum Development Area (JPDA) and outer EEZ security arrangements:
   - Review security arrangements in the JPDA.
   - Clarify the differences between Australia’s maritime safety and security response capabilities and those of neighbouring regional countries such as Timor-Leste and Indonesia and identify the issues that may affect safety and security planning and response arrangements at the outer limits of Australia’s EEZ.

**Onshore security**

In the onshore environment, OTS has responsibility to oversight MTOFSA-regulated maritime and aviation facilities and state and territory police are responsible for the protection of onshore critical infrastructure and response to criminal or law-enforcement related breaches or incidents at all onshore facilities. The onshore facilities involved in oil and gas production and operations include LNG plants, CSG well heads, pipelines, and maritime ports and heliports. Most of these are not subject to specific regulatory oversight or legislative requirements. Similarly, many of the heliports that service offshore facilities and production operations fall outside current aviation security arrangements and are only subject to MTOFSA security requirements plus any additional aviation security measures imposed at the discretion of the operator.

**Single federal incident reporting centre**

From an industry perspective significant doubt continues to exist with regard to the quality and clarity of reporting arrangements. Company representatives gave widely differing accounts of the reporting steps they would take in a given incident situation with most representatives saying they would need to make multiple calls (some as high as 20) before being comfortable that response action would follow. To improve this situation, industry has for some time been calling for an unambiguous single point of contact for all industry compliance and incident response activity.

While oil and gas companies have developed constructive relationships with relevant state and territory police who are likely to be the initial contact point for offshore operators in the event of a security related incident, it is clear that federal reporting arrangements need to be better clarified. The establishment of a single federal point of contact for incident reporting is, on the evidence provided to and considered by the Inquiry, warranted and would significantly improve the effectiveness of current reporting arrangements.

A single federal incident-reporting centre could be situated in a number of locations but the Australian Government Crisis Coordination Centre (AGCCC), located within the Attorney-General’s Department was recognised by most government agencies and industry representatives as the preferred location.

The AGCCC is a 24/7 dedicated ‘all-hazards’ facility that provides ‘whole of government’ situational awareness, coordination of physical assistance, and briefing and support to executive decision makers from across the Australian Government, non-government and state and territory agencies. The National Security Hotline is also a component of the AGCCC Operations Section.
6. RECOMMENDATION

The Inquiry recommends that the Australian Government review the current reporting and command and control arrangements governing security compliance and incident response on offshore oil and gas facilities with a view to improving their clarity and effectiveness.

POSSIBLE OPTIONS:

6.1 Review the current arrangements for command and control of federal, state and territory national counter-terrorism incidents and for reporting suspected security incidents—this will ensure the arrangements are adequately understood by all relevant parties, particularly by stakeholders of the offshore oil and gas resources sector.

6.2 Create a single ‘all-hazards’, triple zero (000) style, federal incident reporting centre for the offshore oil and gas resources sector industry.

6.3 Declare the Australian Government Crisis Coordination Centre (AGCCC) as the single, federal ‘all-hazards’ incident reporting centre for the reporting of offshore safety and security incidents, and with responsibility for:
   - the coordination of immediate response and physical assistance; and
   - the provision of advice and support to executive decision-makers within government and to industry.

Recruitment and vetting

The vetting of Australian employees as part of the application process for a MSIC generally comprises a criminal record check as well as internal company checks deemed appropriate. Industry sees the MSIC process as providing an additional layer of security vetting above that which they can provide themselves. However, although the MISC vetting process provides a security assessment and a photographic record of an individual employee, the process is limited. The MSIC is only intended to identify persons—by photographic identification—who are, based on available information, suitable to work unaccompanied on a regulated facility. Currently, the requirement for a MSIC does not apply to foreign nationals or to Australian and other workers engaged on non-regulated vessels operating under subcontract arrangements.

Companies are increasingly recruiting personnel from overseas due to skill shortages in Australia. Usually, these employees are granted a 457 visa (for professional and skilled migrants), which, again, involves only limited security vetting. The 457 visa is a temporary long-stay work visa under which an applicant must be sponsored by an employer. The employer must meet specific sponsorship and nomination criteria before a visa application will be considered, but these conditions focus on the precise positions desired to be filled by overseas workers and the skills required to perform that work. The overseas workers must then demonstrate they have the skills to meet the requirements of the nominated position.

Although the focus placed on security and criminal vetting is unavoidably restricted, realistically, there is a limit on the extent to which MSIC and work-visa style vetting arrangements could be tightened or extended.
The limitations of normal employee vetting arrangements, however, need to be understood (both by industry and government) in the development and maintenance of an overall integrated security management system.

From an industry perspective, this understanding will be important to ensuring that, as far as possible, any vulnerability created by the limitations of their own company recruitment practices and MSIC style vetting is mitigated by other security arrangements.

Currently, there is a misunderstanding within industry as to precisely what protection MSICs afford. Some companies refer to it as a qualification, while others see it as an accreditation. However, some believe that MSIC provides a broad based security assessment into the background of the MSIC holder.

On 16 June 2011, the Parliamentary Joint Committee on Law Enforcement (PJCLE) tabled the report on its Inquiry into the Adequacy of Aviation and Maritime Security Measures to Combat Serious and Organised Crime at Australia’s airports and seaports. The inquiry includes 22 recommendations on the effectiveness of the current MSIC and ASIC security identification cards in relation to serious and organised crime. Many of these recommendations have relevance to the Offshore Oil and Gas Resources Sector Security Inquiry.

As a consequence, this inquiry team recommends that the PJCLE report be read in conjunction with this report. The PJCLE Report includes an assessment of the effectiveness of the Aviation Security Identification Card (ASIC) and MSIC schemes, including the process of issuing ASICS and MSICS, the monitoring of cards issued, and the storage of, and sharing of, ASIC and MSIC information between appropriate law enforcement agencies. A number of the recommendations contained in the PJCLE report were corroborated during this Inquiry and are listed below for emphasis. The Inquiry considers that, to the extent these recommendations have not yet been implemented, they be further considered for implementation.
PJCLE Recommendations:

Recommendation 10:

4.81 The committee recommends that access to port security areas prescribed under the Maritime Transport and Offshore facilities Security Act 2003 should require verification that the Maritime Security Identification Card belongs to the individual seeking access, either through human gate operators, verification by Closed Circuit Television or any other appropriate solution.

Recommendation 14:

5.45 The committee recommends that the Attorney-General’s Department, in consultation with the Australian Crime Commission, reviews the list of relevant security offences under the ASIC and MSIC schemes to assess whether any further offences are required in order to effectively extend those schemes to protect the aviation and maritime sectors against the threat of infiltration by serious and organised criminal networks.

Recommendation 15:

5.72 The committee recommends that the Attorney-General’s Department arrange for a suitable law enforcement agency to be given the power to revoke an Aviation Security Identification Card or Maritime Security Identification Card if it is determined that a cardholder is not a fit and proper person to hold a card on the basis of compelling criminal intelligence.

Recommendation 16:

5.76 The committee recommends that the MSIC eligibility criteria be harmonised with that of the ASIC scheme so as to make two or more convictions of an individual for maritime security relevant offences grounds for disqualification if one of those convictions occurred in the 12 months prior to an application, regardless of whether either conviction led to a term of imprisonment.

Recommendation 17:

5.94 The committee recommends the expansion of the coverage of the ASIC and MSIC schemes to capture a greater part of the overall supply chain, including some or all of the following:

– Staff at cargo unpacking and stuff-unstuff facilities’
– Transport workers involved in the transmission of cargo between ports, airports and other parts of the logistical chain;
– Customs brokers that do not access port facilities; and
– Human resource staff and management at companies with employees that currently must hold ASICS or MSICs.

A particular point of vulnerability relates to employees engaged under contract and sub-contract arrangements within the oil and gas sector. Under current arrangements, security vetting is likely to have been delegated to the contractor or subcontractor and, where the contracts involve non-regulated vessels or ports, there may be no requirement for employees to hold MSIC authority or to have gone through any specific security vetting process.

In the current expansion of offshore oil and gas exploration, construction and operation, increased numbers of non-regulated support vessels are being taken on contract to support offshore developments. This development reinforces the importance of the assessment of current employee vetting schemes.

7. **RECOMMENDATION**

The Inquiry recommends that a review is conducted of current industry recruitment and vetting processes to identify and clarify their scope, coverage, gaps and limitations and areas for improvement.

**POSSIBLE OPTIONS**

7.1 Initiate and maintain a briefing program to ensure that relevant industry and government representatives have an accurate and comprehensive understanding of the range and scope of Maritime Security Identification Card (MSIC) vetting and assessment and of the reality of the limitations and gaps in the current employee security vetting process.

7.2 Extend the current MSIC security vetting arrangement to cover all operations associated with offshore oil and gas exploration, construction and production activities—for example, to cover

- vessels under 500 gross register tonnage;
- unregulated maritime ports;
- supply chain operations; and
- sub-contractor arrangements.

7.3 Initiate a consultative process between industry and government to develop and agree on mutually desired practices and standards to strengthen employee security.

During the Inquiry process, discussions were held with Interpol concerning the possibility of an industry-Interpol partnership that would allow vetting of prospective overseas workers against Interpol-managed databases.

Communication has been received from Interpol offering to verify the background of potential overseas workers by comparing applicants’ non-nominal data against Interpol’s databases, as well as against other appropriate law-enforcement databases.

It is proposed that after Interpol has ensured that no record exists on these databases, a Globally Verifiable Identity (GV-ID) Card will be issued to the vetted overseas workers. This partnership would operate to enhance the identity management of industry labour, increase its operational security, and assist the law enforcement community in preventing and detecting potential security threats.
Industry has shown an interest in pursuing this offer, which could either be advanced on an individual company-by-company basis or through a collective industry forum or association such as APPEA.

Interpol databases are subject to access limitations and confidentiality protections, and it would be necessary to ensure that relevant privacy considerations would be maintained in any arrangements entered into between a company or association and Interpol. While the current extent of data held by Interpol databases is limited according to the number of member countries that have so far agreed to participate and share data, subscriptions are increasing. Despite the current data limitations, the Interpol proposal is worthy of consideration and would operate to provide another layer in the industry security-vetting process.

20. **Option for the possible use of the Interpol Globally Verifiable Identity (GV-ID) card:**

Companies individually, or through APPEA acting on behalf of the Australian oil and gas resources sector, enter into a partnership with Interpol, under which Interpol would verify background information on potential overseas workers, and issue an Interpol GV-ID card for such workers.

**Training and awareness**

Currently, the only endorsed training programs on security awareness that are in place for the offshore environment are those for company security officers and for ship or facility security officers. These courses are endorsed by OTS and AMSA, as appropriate, but are not currently subject to any formal accreditation.

Accredited training courses, to Certificate II or III standard, are required for maritime security guards and perimeter or site security personnel, but the standards are inconsistent and, in some areas deficient. In particular, the Inquiry noted that some security guards were not conversant with the testing and use of screening equipment and their powers as a Maritime Security Guard (MSG) under MTOFSA.

There is no broader industry-wide, accredited security training program, nor are there security induction or awareness courses that are suitable to be delivered to new offshore facility employees. Any such awareness programs are conducted voluntarily and solely at the discretion of an individual company or operator.

In April 2010 OTS produced a Guidance Paper on Competencies for Maritime Security Guards (Baseline Qualifications). The guidance paper outlines the specific additional powers of a MSG and the maritime industry participant’s compliance obligations with the regulatory requirements for MSGs. A list of competencies, intended as guidance for use by industry to develop or source the appropriate training for MSGs, is included in the Guidance paper.

As the experience of the 2004 London underground bombings and serious incidents in other countries has demonstrated, even in a large metropolitan area, it is likely to take formal emergency response resources about 20 minutes to arrive and take charge at the scene of an incident.

In offshore and many onshore LNG and other oil and gas situations, the more isolated location of the infrastructure is likely to significantly extend this response timeframe. In many offshore safety or security incident situations the ability of police to immediately or effectively respond to an incident may not be guaranteed.
An inevitable consequence is that the first response to offshore or onshore safety or security incidents will, in many situations, rest with on-site employees. While the role and capacity of any such response will obviously depend on the circumstances of the incident, this reality needs to be recognised and addressed in any industry contingency planning.

Equally importantly, particularly given the hydrocarbon-rich environment of oil and gas operations, is the need to equip employees with the basic skills and knowledge required to identify and react to any suspicious or unusual behaviour that may indicate an intention to commit a dangerous or disruptive act.

Within the UK rail system, targeted awareness education programs—aimed at encouraging and enabling relevant staff to make judgment calls on what is or is not suspicious—are delivered to all staff who work in areas of risk. These programs, apart from covering a range of safety and evacuation-related procedures also include information on maintaining business continuity, the dangers of over-reaction through incorrect diagnosis and complacency.

The Inquiry found that onshore security-awareness training in Australia varied between companies and between facilities in the same company. Training ranged from a security-awareness component within site-induction programs for employees and visitors to little or no training at all.

As an example, most safety-awareness video presentations before helicopter flights did not include a security-awareness component. Where a security component was included in the video presentation, reference was made to MTOFSA security requirements for offshore facilities.

The Inquiry team witnessed several safety-related exercises on offshore facilities. These tested a wide range of safety-related scenarios and procedures, including communications and the knowledge levels of relevant staff. One of the inquiry team’s observations was that many staff were unfamiliar with their responsibility to preserve the incident scene.

8. **RECOMMENDATION**

The Inquiry recommends that the Australian Government assist industry with identifying and implementing appropriate minimum-standard security training and awareness programs sufficient to equip facility staff with the skills and understandings necessary to competently respond to security-related threats and situations should they arise.

**POSSIBLE OPTIONS:**

8.1 Settle mutually-agreed minimum benchmark standards for the frequency and measurement of staff security induction and refresher training on facilities, through discussions between relevant government agencies and industry stakeholders - this will ensure that relevant facility staff possess and maintain adequate levels of skill and knowledge.

8.2 Develop short awareness-training programs that are sufficient to:

- provide selected facility workers with advice on how best to identify, report and respond to suspicious or unusual behaviour, sightings or incidents; and

- ensure selected facility workers have a realistic, practical working knowledge of existing security plans and arrangements and their immediate-response responsibilities.
8.3 Review the current Maritime Security Guard (MSG) training framework, through joint industry and government initiatives to ensure that:

- relevant training programs adequately meet required security standards; and
- the training programs provide MSGs with an adequate understanding of the powers and authorities they possess under MTOFSA, and how they should be lawfully exercised.

8.4 Develop a training program for immediate-responder crime scene protection to be delivered to selected facility staff that would:

- provide guidance on how to determine, contain and protect a likely crime scene, so as to assist any criminal investigation that may follow;
- explain the importance where items or people within a crime scene are required to be moved for safety or medical reasons, of recording the original position of the item or person, and provide guidance on the evidential value of avoiding any unnecessary interference with anything within a crime scene; and
- provide guidance on the type of observations or actions that should be reported and recorded at the earliest opportunity.

8.5 Consider providing the above training courses for development under the Australian Quality Training Framework (AQTF) to serve as a national security training and assessment process to achieve industry wide accreditation consistency.

8.6 Consider the Australian National Security College as a possible training facility that industry can access on a cost-recovery basis.

Cyber security

‘The critical infrastructure that underpins our daily lives increasingly depends on hyper-connected online systems. While significant resources have historically been needed to cause devastating consequences for geopolitical or corporate powers, it is increasingly possible for skilled individuals to do so remotely and anonymously through networked computer systems’.

From The Dark Side of Connectivity, Global Risks Report 2012

Cyber security including the protection of information and the integrity of operating systems is an increasingly serious issue for offshore oil and gas operations and facilities. Cyber attack can be used to cause disruption to computer systems and networks through the denial of essential services and systems, or implanting of viruses to degrade or stop functionality of computer programs and systems. Cyber attacks can also be used to obtain commercial information through active searching of databases or through background collection and download of data, to steal data for criminal purposes, or even for espionage for state-related purposes.⁶²
Despite the cost efficiency and logistic advantages of the use of remotely controlled SCADA type systems, the reliance on external supervisory control of facilities creates new and additional threats, which need to be understood and mitigated.

SCADA generally refers to industrial control systems that monitor and control industrial processes. A SCADA system usually consists of a human operator monitoring and controlling a process or processes; a supervisory computer system, gathering data on the process and sending commands to the process; remote terminal units connecting to sensors in the process; converting sensor signals to digital data and sending digital data to the supervisory system.

Modern industry SCADA control systems are powerful enough to cause damage to or destroy the plant they are monitoring and controlling. SCADA devices and controllers are normally only functionally tested for what the devices are supposed to do—they are not tested for what they should not be able to do. This is what a hacker may exploit to gain control of the system and potentially stop an operation, damage or destroy equipment, or interfere with a process. SCADA systems are currently frequently built and operated with insufficient attention to security vulnerabilities. As a consequence, systems can be infiltrated by unauthorised external connections that make it vulnerable to cyber attack.

Within the Australian environment, the oil and gas industry is moving further offshore in its search for new oil and gas fields, using new technology to reduce costs and improve the commercial viability of such deepwater production. At the same time, the continued advancement of technology is increasing the capacity of companies to operate remote, unmanned offshore facilities and subsea operations, particularly in those more remote offshore locations within the Australian EEZ where transport and manning costs pose the most challenges.

Companies expend considerable effort and capital to keep abreast of cyber threats and must achieve the maximum level of computer security to protect information and processes, while allowing the very same information and processes to remain accessible for the ongoing operation of company business. To illustrate the cyber threat potential, an international example was provided where 40,000 hits per hour and 600 viruses were detected and 41 firewall levels were penetrated within a period of a month. A leading anti-virus development company has estimated that around 100,000 new malware are produced worldwide each day. This shows that the difficulty to identify the source of a cyber attack and related embedded malware together with the challenges of managing and controlling the impacts caused by an intrusion have the potential to combine and cause the complete shutdown of a major national or global corporation.

As an example, Stuxnet, which is considered the first discovered malware that spied on and subverted industrial systems, spread indiscriminately around the world, with its highly specialised malware payload only targeting the systems it was designed to monitor and control. Stuxnet is a denial-of-service type cyber attack against specific designated targets and is a weapon that can easily target the SCADA systems on which a state and its industrial infrastructure depends.

A more recent example of this type of cyber attack is Night Dragon, which operated to infiltrate critical infrastructure, exposing underlying weaknesses in business IT systems. Night Dragon attackers targeted global oil, energy, and petrochemical companies, with the apparent intent of stealing sensitive information such as operational details, exploration research, and financial data.
A campaign of cyber attacks, targeting US natural gas pipeline operators, which was identified in early 2012, also raised security concerns about vulnerabilities in key infrastructure. The attacks apparently involved sophisticated spear-phishing activities that targeted specific personnel within companies or organisations by sending fake emails designed to encourage employees to divulge passwords and other security information.

An alert from the US Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (the US equivalent of Australia’s CERT) identified the emails as ‘convincingly crafted to appear as though they were sent from a trusted member internal to the organisation’. According to US security experts these attacks highlighted the vulnerability of critical infrastructure systems, including control systems within electrical grids, water utilities and pipeline operations. Additionally, the potential for flow on interdependency threats was identified with the biggest fear being that a ‘coordinated attack on several facilities (sic) would trigger automatic responses at other facilities, potentially causing a chained effect similar to an electrical black out, but with more severe consequences’.

The above attacks demonstrate the importance of robust cyber-security plans that are sufficient to resist actions by experienced and professional hackers as well as accidental intrusion and amateur hacking. The World Economic Forum, in its Global Risks 2012 Report, lists cyber attacks as the 4th most likely global risk for 2012.

The need to create strong internal information-system security awareness and operating protocols is even more important when considering the new generation of potential employees growing up in a cyber world. In this cyber world, a person who feels anonymous and concealed is more likely to commit acts, or reveal information, that they would never contemplate in the physical world.

Organisations are changing from a machine-based, internally-focused structure to a more open structure with stronger external relationships that are more interconnected and use multi-layered IT networks. This means that existing information technology and industrial control system security practices face challenges in meeting and managing future cyber security demands. The ability to access information is currently ahead of the ability to control such access and the danger exists that current industry-compliance standards may not identify and mitigate all emerging threats. Therefore, there is a need within the offshore industry, and the broader community, to understand the impact of the increasing utilisation of, and dependency upon, information systems.

The importance of senior executives within the oil and gas industry being part of this education program cannot be overstated. Companies are unlikely to respond effectively to cyber threat challenges unless the organisation’s executives have an adequate understanding of the various threat vectors and the likelihood, risks and consequences of cyber attacks. Within the US and UK, executive level cyber security training programs have been developed that offer short, intensive courses aimed at fast-tracking executives to a level of understanding sufficient to identify what is real and what is simply hype with regard to cyber threats. It is considered that these types of programs would also be beneficial to executives and security chiefs operating within the Australian offshore and onshore oil and gas environment.

As the number of users connected to the internet and the reliance on online data, continue to increase, the difficulties and importance of attaining and maintaining adequate and effective IT security control grows exponentially.

Within the Australian environment the Computer Emergency Response Team (CERT) has primary responsibility as the initial point of contact for cyber security incidents impacting upon Australian networks and for providing assistance in the protection of systems from cyber intrusion.
CERT works closely with the private sector to identify critical infrastructure and systems that are important to Australia’s national interest. Risk based assessments provide government and private organisations with information and guidance to assist in the protection of information and communication technology infrastructure from cyber intrusion. These are complemented by trusted information exchanges between the Australian Government and Australian businesses on cyber security issues.

The CERT Australia website <www.cert.gov.au> contains useful and up to date information on cyber threats and the CERT Strategies to Mitigate Targeted Cyber Intrusions paper (21 July 2011) can be found at <http://www.cert.gov.au/www/cert/cert.nsf/Page/Alerts_and_Advisories >

Additionally, the Cyber Security Operations Centre (CSOC), established in the Defence Signals Directorate (DSD) as an initiative of the Australian Government’s Defence White Paper to mitigate the cyber threat to Australia’s national security, aims to provide guidance to government on sophisticated cyber threats against Australian interests.

9. RECOMMENDATION

The Inquiry recommends that senior executive of oil and gas companies operating within the Australian environment:

– consider participating in executive cyber security training programs to ensure they have an appropriate level of understanding of the reality of the emerging cyber threat environment to business integrity and continuity;

– implement measures to ensure there is an appropriate level of understanding, at both the executive and operational levels, of the potential damage that may be caused to their business by cyber intrusion and take active steps to identify:

  – the information most critical to business continuity and integrity;
  – the critical risks associated with any unlawful access to information; and
  – the most effective way to achieve a balance between maintaining maximum levels of computer security and protection of information while facilitating the access to information necessary for efficient business operations.

10. RECOMMENDATION

The Inquiry recommends that to assist the above process the Australian Government facilitates periodic

– Computer Emergency Response Team (CERT) presentations at OGSF, Energy Security Group (ESG) and similar forums; and

– Cyber-based exercises, targeted directly on offshore oil and gas operations with industry.
Case study

The Montara oil spill

One of Australia’s worst oil spills began with a small ‘burp’ of oil and gas issuing from the H1 Well at the Montara Well Head Platform in the early hours of 21 August 2009. Two hours later, a kick expelled a column of oil and gas, which continued unchecked for over 10 weeks.

Thankfully, the sixty-nine workers on the rig were safely evacuated and there were no injuries or fatalities. However, the environment suffered as a slick began to spread across the Timor Sea approximately 250 kilometres off the northwest coast of Australia. Estimates of the amount of oil released range from 400 to 2,000 barrels per day and the Report of the Montara Commission of Inquiry said that, ‘weathered oil could have affected, at various times, an area as large as 90,000 square kilometres’.

The commission’s report was a scathing indictment of both the operator and the regulator. It said that PTTEP Australasia (Ashmore Cartier) Pty Ltd (PTTEPAA) had made a number of critical mistakes. The most serious of these mistakes was the failure to test the integrity of the well’s cement casing when drilling was suspended for five months immediately before the blow-out. Also two ‘pressure containment and corrosion’ well caps were mistakenly left off after instructions to install them were wiped off a whiteboard.

The causes of the disaster were directly attributed to the failure of PTTEPAA to observe ‘sensible oilfield practices’ or even comply with its own well-construction standards. The company’s systemic failures included an inadequate well-operations management plan; senior personnel with limited experience; ambiguous well-construction standards and deficient decision-making in relation to a number of important matters.

The report concluded that an insufficiently diligent regulator, the Northern Territory Department of Resources had also contributed to the disaster by adopting, ‘a minimalist approach to its regulatory responsibilities’ that compounded the company’s systemic shortcomings. As the report said, ‘The regulatory dog did not bark.’

Like the Deepwater Horizon disaster, the Montara disaster dramatically illustrates the devastating consequences of an incident on an offshore facility. The Montara disaster could have been prevented if both the operator and the regulator had exercised due diligence. However, whether an incident be due to accident, negligence or deliberate sabotage, the challenge for industry and government, is to develop a safety and security regime that effectively minimises the risks. In particular, a regime that is clearly articulated, can be clearly understood and is enforceable, when necessary.

The incident emphasises the importance of ongoing reviews and on-site audit inspections, including by government agencies, of safety and security arrangements that can identify and remedy flaws, deficiencies and vulnerabilities where they exist.

The causes of the incident, whilst accidental, could as easily have been the result of deliberate action and intent, particularly in the absence of any effective oversight or management planning. This further reinforces the importance of the external audit process.
Conclusion

As mentioned at the start of this report, the security arrangements in place for offshore oil and gas infrastructure within Australia’s EEZ generally reflect those in place in other similar locations around the world.

Many countries and companies are facing challenges similar to those identified within Australian waters. Indeed, in each country visited by the Inquiry, local authorities and governments were subjecting their oil and gas resources sector to ongoing evaluation, with the aim of continuing to improve the quality of security preparedness and risk mitigation.

When considering the recommendations and options identified in this report, it is important to recognise that in the countries visited, the creation and maintenance of a comprehensive and effective security regime remains work in progress.

Similarly, within the Australian jurisdiction, despite the progress made in developing an offshore security regime, the Inquiry identified areas of vulnerability in current security practices and arrangements that are considered sufficiently serious to warrant early attention and improvement.

In assessing the importance and relevance of these issues, the Inquiry has essentially placed an emphasis on vulnerability and consequence rather than threat. This is not to suggest that threat and threat assessment are not integral to any security management program but, rather, to emphasise that:

- even if no specific immediate threat has been identified, threats to oil and gas infrastructure still exist; and
- to achieve effective levels of security preparedness these threats need to be analysed through the lens of vulnerability and consequence.

In the opinion of the Inquiry, an effective security management framework is only likely to be achieved and maintained if there is a recognition that threats potentially exist at every facility. Therefore, site-specific vulnerability assessments need to form the basis of determining preventive measures and evaluating preparedness and counter measures.

In assessing the significance of individual areas of vulnerability, it is also important to recognise and understand the interdependencies between upstream oil and gas production activity and downstream energy production and supply.

The offshore oil and gas production industry is essentially at the front end of an energy chain that has proven to be as strong as its weakest link. The impact on Western Australian energy supplies from the Varanus pipeline gas leak in 2008, which reduced the Western Australian gas supply by about a third, illustrates this.
However, while the nature of offshore operations makes it difficult to eradicate or mitigate all vulnerabilities, these can be identified so that measures to reduce the level of risk and improve operational resilience can be implemented.

This report does not seek to provide a prescriptive report card on the state of security effectiveness and preparedness in the oil and gas resources sector environment. Rather, in accordance with the provisions of the Inspector of Transport Security Act 2006, it attempts to offer impartial and, hopefully, constructive advice to industry and government stakeholders that may be of value in the further and ongoing review and improvement of offshore oil and gas industry security measures. Indeed, when considering and responding to any of the recommendations and options contained in this report, industry and government will be operating from a strong and constructive basis. Despite the issues identified in this report, the nature and quality of the relationships between government and industry are strong and continue to improve.

All companies operating within Australian waters that have worked with the Inquiry have indicated support for the recommendations and options identified by the Inquiry. Additionally, a number of government agencies are already, quite separately and independently, implementing a range of initiatives that expressly focus on the issues of concern raised in this report.

These initiatives include the high level industry forum convened by ASIO in March 2012, the discussions currently occurring between the ADF and offshore oil and gas companies regarding active exercising, the review of VTS and shipping fairways by AMSA, the OTS involvement in an assessment of the current MSIC arrangements, and the consideration currently being given to broadening and further strengthening the value of OGSF, TISN and other related forums.

During Inquiry discussions with government agencies, a view was put that this Inquiry report should not seek to make recommendations, but rather should identify desired outcomes and options by which these outcomes may be achieved.

The Inquiry understands and respects this view, and carefully considered this suggestion. However, considering the range and interdependency of identified issues of concern and the requirements under the Act to provide the Minister with a final report that includes conclusions and recommendations, the Inquiry decided that recommendations should be made in regard to areas of primary concern.
Pursuant to subsection 11(1) of the Inspector of Transport Security Act 2006 (the Act), the Minister for Infrastructure and Transport, the Honourable Anthony Albanese MP, directs the Inspector of Transport Security (the Inspector) to conduct an inquiry into the Offshore Oil and Gas Resources Sector Security to assess the quality and effectiveness of current security arrangements in place and response capabilities of resource operators and government to a security incident or an attack on offshore oil and gas exploration and production infrastructure.

The ‘Terms of Reference’ issued by the Minister primarily require the Inspector to inquire into and:

- review and assess both the onshore and offshore government and industry relationships and arrangements relevant to the security of offshore oil and gas platforms and broader related infrastructure;
- review the effectiveness of current stakeholder/government agency communications and coordination capabilities;
- review the nature and extent of current security control and oversight arrangements, including arrangements currently in place to monitor the sea areas around offshore oil and gas exploration, production and offload platforms and facilities, pipelines and shore based offload and support facilities;
- review the ability of security regulated offshore facility, port, port facility and ship operators and owners to undertake risk assessments and develop and implement security programs as required under Commonwealth Legislation and International Conventions and Codes;
- review and assess whether current security measures and arrangements are contributing to positive security outcomes in the national interest;
- review and identify any sea and landside security gaps and weaknesses and areas for improvement;
- review the potential consequences and likelihood that may flow from a violent takeover of any offshore oil or gas infrastructure in economic, environmental and human cost terms; and
- review the coastal and high seas shipping routes used in the transport of oil and gas products, the supply and support of offshore platforms and facilities used in the delivery of construction components for offshore oil and gas field development to identify any potential security risks to such transport or infrastructure.
As part of the Inquiry the Inspector shall consider the following:

- the impact of an incident or attack on the industry sector, including business recovery and the environment;
- the security implications of foreign shipping and crews that approach and access offshore gas or oil platforms and facilities;
- the intergovernmental and industry issues involved in responding to an incident against an offshore oil or gas platform or facility, or a safety of life at sea incident involving offshore gas and oil platforms, facilities or support vessels;
- the current whole-of-government approach to offshore oil and gas infrastructure security and identify, where relevant, areas for improvement;
- the clarity and effectiveness of government lead agency responsibilities to respond to an incident and under what circumstances, and their capacity to meet required security response outcomes;
- the resources government or industry may require to respond to an incident or attack involving offshore oil and gas infrastructure;
- the current industry security arrangements, including the extent, type and effectiveness of security training, assessment, drills and exercise regimes in place within the offshore oil and gas sector, to ensure they are relevant and necessary to the risk profile; and
- security information provided to industry by Commonwealth agencies.

The Inspector of Transport Security Act 2006 provides a framework for the Inspector to conduct independent ‘no-blame’ inquiries and make recommendations in relation to transport security matters and offshore security matters, in order to better contribute to the improvement of transport security and the security of offshore facilities. The Act also provides the Inspector with the powers to perform his duties, the means to protect information gathered during an inquiry and immunities from prosecution for those who cooperate with his inquiries.

Administrative support for the Inquiry will be undertaken by the Office of the Inspector of Transport Security.
APPENDIX 2: International offshore and onshore site visits and consultations

Offshore and onshore site visits

United States
United States Coast Guard, Eighth Coast Guard District Headquarters, New Orleans, Louisiana
United States Coast Guard, Marine Safety Unit, Morgan City, Louisiana
EnSCO 8502, deepwater, semi-submersible drill rig, Gulf of Mexico
Louisiana Offshore Oil Port, offshore control and pumping platforms, Gulf of Mexico
Louisiana Offshore Oil Port, control and security centre, Galliano Louisiana
ERA heliport, Fourchon, Louisiana
PHI heliport, Boothville, Louisiana

Consultations

United States
United States Coast Guard, National Headquarters, Washington
Government Accountability Office, Washington
Bureau of Ocean Energy Management, Regulation and Enforcement, Washington
American Petroleum Institute, Washington
Australian Embassy, Washington
United States Coast Guard, Boston
United States Coast Guard, Eighth District HQ, New Orleans
Apache, Houston
BHP Billiton, Houston
BP, Houston
Chevron, Houston
ConocoPhillips, Houston
ENI, Houston
ExxonMobil, Houston
Shell, Houston
United Kingdom
Grampian Police
Centre for the Protection of National Infrastructure, London
Department of Energy and Climate Change, London
Home Office, London
State of Service Representative for Maritime Salvage and Intervention, London
Maritime and Coastguard Agency, London
Royal Navy, London
National Maritime Intelligence Centre, London
Apache North Sea Ltd, Aberdeen
BP, London
Chevron, London
Oil Companies International Marine Forum, London
Society of International Gas Tanker and Terminal Operators, London
Oil and Gas Cyber Security Conference 2011, Kensington, London
Australian High Commission, London

France
INTERPOL, Lyon
International Association of Oil and Gas Producers, Paris
Total, Paris
Perenco, Paris

Norway
Ministry of Petroleum and Energy, Oslo
Ministry of Defence, Oslo
Petroleum Safety Authority Norway, Stavanger
Rogaland Police, Stavanger
Eni Norge, Stavanger
Norwegian Oil Industry Association, Stavanger

Timor Leste
CHC helicopters, Dili International Airport

Indonesia
Deputy for Infrastructure and Logistics, Indonesian Ministry of State Enterprises, Jakarta
BPMIGAS, Ministry of Energy and Mineral Resources, Jakarta
Indonesian Sea and Coast Guard, Jakarta
BP, Jakarta
SANTOS, Jakarta
Australian Embassy, Jakarta

Philippines
Philippine Coast Guard, Headquarters, Manila
Philippine National Police, Maritime, Camp Crame, Quezon City
Philippine Navy, Headquarters, Naval Station Jose V Andra, Manila
Australian Embassy, Manila
APPENDIX 3:
Australian offshore and onshore site visits and consultations

Offshore and onshore site visits

Western Australia
Woodside, Facility Fly-over NWS offshore facilities
Woodside, Karratha LNG plant, Burrup Peninsula
Woodside, Pluto LNG plant, Burrup Peninsula
Woodside, King Bay supply base, Port of Dampier
Woodside, Northern Endeavour FPSO, Browse Basin
Dampier Port Control, Dampier Port Authority
CHC Helicopters, Karratha Airport
Bristow Helicopters, Karratha Airport
CHC Helicopters, Truscott Airbase
Shore Air, Truscott Airbase
Apache Energy, STAG offshore production platform
Apache Energy, Harriet Joint Venture and John Brookes Joint Venture Oil and Gas Production Facilities, Varanus Island
Apache Energy, Varanus Island heliport facilities
Chevron Australia, Barrow Island airport facilities
Chevron Australia, WAPET oil production facilities, Barrow Island
Chevron Australia, Gorgon Project, Barrow Island
Cobham Aviation airport facilities, Perth Airport

Northern Territory
Conoco Phillips LNG Plant, Wickham Point, Darwin Harbour
Darwin Port Control, Darwin Port Corporation, Darwin Harbour
Pearl Aviation, Darwin Airport

Joint Petroleum Development Area (Timor Sea)
Conoco Phillips, Liberdade FSO, Bayu-Undan oil field, JPDA
Conoco Phillips, fly-over Bayu-Undan oil field offshore facilities, JPDA
Queensland
Santos CSG LNG plant construction site, Curtis Island, Gladstone Harbour
Conoco Phillips CSG LNG plant construction site, Curtis Island, Gladstone Harbour

Victoria
Exxon Mobil gas processing and crude oil stabilisation plant, Longford, Victoria
Exxon Mobil heliport, Longford, Victoria
Exxon Mobil Cobia offshore production platform, Bass Strait
Exxon Mobil West Tuna offshore production platform, Bass Strait
Exxon Mobil Barry Beach marine terminal, Welshpool, Victoria

Australian Capital Territory
Australian Maritime Safety Authority, Rescue Coordination Centre, Canberra
Emergency Management Australia, Crisis Coordination Centre, Canberra
Attorney-General’s Crisis Coordination Centre

Consultations
Australian Capital Territory
National Security Advisor
Department of Resources, Energy and Tourism
Australian Federal Police
Australian Maritime Safety Authority
Department of Sustainability, Environment, Water, Population and Communities
Oil and Gas Security Forum
Australian Petroleum Production and Exploration Association
Border Protection Command
Department of Defence
Attorney-General’s Department
Office of Transport Security, Department of Infrastructure and Transport

Western Australia
Australian Petroleum Production and Exploration Association
Oil and Gas Industry Security Managers Meeting
Woodside Perth and Karratha
Pilbara Security Forum, Karratha
Western Australia Police, Perth and Karratha
Fire and Emergency Services Authority, Regional Headquarters, Karratha
Apache Energy
Inpex
IALES
Chevron Australia
National Offshore Petroleum Safety Authority
National Offshore Petroleum Safety and Environmental Management Authority
International Offshore Petroleum Regulators and Operators Summit
Future Directions
Go Marine Group
Offshore Marine Services
Samson Express Offshore
Vermilion Oil and Gas Australia

**Northern Territory**
Oil and Gas Security Forum, Darwin
Energy Security Group
ConocoPhillips
Darwin Port Authority
Svitzer Australasia and Coastal Tug and Barge
Workboats Northern Australia

**Victoria**
Oil and Gas Security Forum, Melbourne
ExxonMobil
Australian Marine Oil Spill Centre Pty Ltd
Emergency Policy and Strategy Co-ordination, Department of Primary Industries
Policy and Compliance, Security and Emergency Management, Department of Transport
Critical Infrastructure Protection Unit, State Emergencies and Security Department, Victorian Police

**South Australia**
Santos

**Queensland**
University of Queensland
SANTOS, Brisbane and Gladstone
ConocoPhillips, Brisbane and Gladstone
Gladstone Port Authority
Queensland Police, Water Police, Gladstone
Joint Agencies Maritime Advisory Group
Mining and Petroleum, Department of Employment, Economic Development and Innovation
Mines and Energy, Department of Employment, Economic Development and Innovation
APPENDIX 4: Summary of current and proposed Australian oil and gas operations

Northern Territory/Joint Petroleum Development Area

The Northern Territory currently has one Darwin based LNG production and export facility using gas piped from the JPDA area in the Timor Sea. Another Darwin LNG plant is at the design stage. Darwin domestic electricity uses natural gas energy supply by pipeline from the Bonaparte Basin.

Bayu-Undan/Darwin LNG

The Darwin LNG plant converts gas from the Bayu-Undan field in the JPDA area of the Timor Sea into LNG for sale to Tokyo Electric and Tokyo Gas in Japan. The Bayu-Undan gas field consists of a manned central production and processing platform complex, a remote platform, an FPSO and a 502 kilometre gas pipeline connection to Darwin. The FPSO processes, stores and offloads oil condensate and LPG. The Darwin plant at Wickham Point, Darwin produces some 3.5 million tonnes per annum of LNG for export. The first shipment of LNG was loaded in 2006.

Blacktip Field

In September 2009, Eni Australia delivered its first gas to Darwin from the Blacktip Project. The Blacktip gas field, 100 per cent owned and operated by Eni, is located in the offshore Bonaparte Basin area of Western Australia approximately 110 kilometres from the onshore processing facility at Yelcherr, near Wadeye in the Northern Territory. Processed gas is transported via a 280 kilometre onshore pipeline from Wadeye to Darwin to the NT Power Water Corporation for use in generating electricity for the Northern Territory. From 1 January 2012, the Blacktip field will produce 100 per cent of the gas for the Northern Territory’s power supply.

Kitan

Eni is Operator of the Kitan Project (with 40 per cent equity) with joint venture partners INPEX Timor Sea Limited (35 per cent) and Talisman Resources (JPDA06-105) Pty Ltd (25 per cent). The Kitan field is approximately 240 kilometres south of the Timor-Leste capital of Dili and 547 kilometres north of Darwin, Australia in the JPDA between Australia and Timor-Leste. Kitan was discovered in February 2008, and in April of that year commercial declaration was made. The field will be produced from three subsea wells and processed by the FPSO “Glas Dowr” operated by Bluewater NV, under contract to Eni. First production is expected in early fourth quarter 2011.

The following is a list of major oil and gas projects in the Northern Territory, including those under development or at project definition stage.
In development

Inpex Ichthys field

Participants: Inpex (Operator – 76 per cent) and Total E&P Australia (24 per cent) Corporation

Location: Middle Arm Peninsula at Blaydin Point in Darwin Harbour, and offshore Darwin

Timeframe: Final investment decision expected in 2010 and first LNG shipment scheduled for 2015

Investment: US$25 billion

Status: The Project is currently in Front End Engineering Design - the project development phase in which plans for the onshore and offshore facilities are defined, designed and evaluated in more detail. The Offshore FEED contract involves engineering work for the Semi-submersible Central Processing Facility (CPF), FPSO unit for condensate treatment and storage, Umbilicals, risers and flow lines and 885km export pipeline to Darwin. The onshore FEED contract involves engineering work for two LNG trains with a capacity of 8.4 million tonnes per annum, LPG and condensate processing plants, storage tanks for LNG, LPG and condensate, administration facilities, utilities and services, power generation infrastructure and a product offloading jetty. The Central Processing Facility will be one of the largest semi-submersible platforms in the world.

QUEENSLAND

In development

The CSG to LNG conversion development activity is predominantly on, or near, Curtis Island, within the port of Gladstone. There are now four major projects either underway or close to a final investment decision for this area.

GLADSTONE LNG PROJECT

Participants: Santos (Operator – 30 per cent), PETRONAS (27.5 per cent), Total (27.5 per cent) and KOGAS (15 per cent).

Location: Gladstone

Timeframe: FID expected in mid 2010 and first gas production expected for mid 2014

Investment: $7.7 billion

Status: The project was approved for construction in early 2011. Work is already underway at GLNG’s mainland sites in the Port of Gladstone with the construction of the temporary and permanent logistics facilities. The LNG plant will initially produce 7.8 million tonnes per annum of LNG, with a maximum potential production of 10 million tonnes per annum.

The project is a partnership between Santos, Australia’s largest domestic gas producer, PETRONAS, Malaysia’s national oil and gas company and the second largest LNG producer in the world, French energy major, Total, the world’s fifth largest publicly traded integrated international oil and gas company, and KOGAS, the world’s largest buyer of LNG.
**CURTIS LNG PROJECT**

**Participants:** Alliance between Queensland Gas Company Ltd of Australia and BG Group plc UK.

**Location:** Gladstone, Queensland

**Timeframe:** Approved and construction underway, with first LNG production scheduled for the end of 2013. Bechtel has been appointed as the project contractor.

**Investment:** Estimated $8 billion

**Status:** The project will involve the expansion of Queensland Gas Company’s Surat Basin gas production operations near Chinchilla, the development of a new 380 kilometre pipeline to Gladstone (central Queensland coast) and the construction of a LNG export facility at Curtis Island, near Gladstone.

**FISHERMAN'S LANDING LNG**

**Operators:** Arrow Energy

**Location:** Fishermand’s Landing Wharf, Gladstone

**Timeframe:** Expected life of 25 years, with construction proposed to commence in 2011 and first production scheduled for 2012.

**Status:** The proposed Arrow LNG Plant Project on Curtis Island will be supplied with CSG from Arrow Energy reserves located in the Surat Basin in South East Queensland and the Bowen Basin in Central Queensland. The liquefaction facility will produce up to 16 million tonnes per annum of LNG, and includes the phased construction of up to four trains or processing plants on its Curtis Island site. Stage 1 includes the construction of two trains of around 4 million tonnes per annum of LNG each.

**AUSTRALIA PACIFIC LNG**

**Participants:** Origin Energy and ConocoPhillips form Australia Pacific LNG (APLNG)

**Location:** Laird Point on Curtis Island in Gladstone, Queensland

**Timeframe:** Final investment decision for Train 1 is expected in 2011 with first production in 2014

**Investment:** $35 billion total development

**Status:** Australia Pacific LNG intends to develop Australia’s largest CSG reserves base into a LNG facility with 14 to 18 million tonnes per annum LNG capacity. The project includes the construction of a gas transmission pipeline 450 kilometre long from the CSG fields to the LNG facility at Curtis Island, off the coast of Gladstone. The project will deliver an additional Australian LNG hub, serving Asia-Pacific and other international markets.
VICTORIA

Victoria is a major contributor to Australian oil and gas production, with potential for further exploration and development. Each year gas produced offshore in Victoria is worth about AUD$1.5 billion, and crude oil production is valued at over AUD$2 billion.

More than 80 per cent of eastern Australian conventional gas reserves are located in the waters between Victoria and Tasmania (Bass Strait), the majority within the Gippsland Basin offshore from Victoria. Gippsland Basin remaining developed liquids reserves are estimated at about 400 million barrels and gas reserves are estimated at seven trillion cubic feet. In the Otway Basin, reserves are estimated at one trillion cubic feet. In Tasmanian administered waters, gas to be produced through Victorian facilities is estimated also at one trillion cubic feet.

Bass Strait reservoirs are expected to produce crude oil and natural gas until at least 2030.

Bass Strait

**Exxon Mobil - Eastern Bass Strait offshore fields** The Eastern Bass Strait offshore fields currently have 23 producing offshore platforms in Bass Strait with pipelines to the Longford gas plant. The Longford plant delivers oil and natural gas by 220 kilometre pipelines to the Long Island processing plant, which has LPG and crude oil storage for ship tanker delivery. Further pipelines supply natural gas to the Victorian domestic gas network or crude oil to Altona and Geelong refineries for further processing. Local demand now absorbs approximately 65 per cent of Bass Strait LPG supply. Since 1969 over 3.5 billion barrels of crude oil and 5 trillion feet of gas have been produced. Total expenditure to date is $12.5 billion.

**Basker/Manta/Gummy offshore oil fields** The project was the first development to utilise an FPSO vessel, the Crystal Ocean, in south east Australia, together with the shuttle tanker Basker Spirit. The small sized FPSO processed oil from the production well subsea manifolds. The tanker delivered the crude oil to Australian refineries. Oil reserves are estimated at 39.8 million barrels. First oil was delivered in 2006 and anticipated operating life is 15 years. In 2011 Beach Energy, as operator, went into a non-production phase and the FPSO was demobilised and removed from the field.

**Yolla offshore field** Yolla field is located in mid Bass Strait between Victoria and Tasmania and is producing gas and oil through two wells and piped 150 kilometre ashore to the Lang Lang processing plant. The gas is delivered to the Victorian Principal Gas Transmission Pipeline for domestic and industrial use.

**Longtom offshore field** Gas from this field is produced via subsea wells linked by pipeline to the Santos-owned and operated Patricia-Baleen gas facility near Orbost in south-eastern Victoria. Sales gas is then transported to the Jemena Eastern Gas Pipeline and condensate to the Shell Geelong Refinery for processing.

**Otway Basin**

**Thylacine and Geographe offshore gas fields** These fields are located some 60 to 70 kilometre off the west Victorian coast and supply gas to a Port Campbell gas processing facility. The gas supplies the Victorian SouthWest Pipeline system for domestic and industrial use. The project is expected to produce 950 billion cubic feet of gas, 12.2 million barrels of condensate, and 1.7 million tonnes of LPG over its life. $1.1 billion development cost.
Minerva oil and gas field The field consists of two subsea wells connected via undersea pipelines some 10 kilometre to shore for processing. The field produces some 135 terajoules of gas and 550 barrels of condensate per day. $225 million cost of development.

Casino gas field The field has two wells supplying gas via a 50 kilometre pipeline to the Iona gas processing plant near Port Campbell Victoria. The plant is connected to the Victorian gas transmission system via the SouthWest Pipeline and the Seagas Pipeline into South Australia. The Henry and Martha gas fields are tied back by undersea wells and pipelines to the Casino wellhead to boost gas production. $200 million cost of development.

In development

**KIPPER**

Participants: Esso Australia, Santos Limited and BHP Billiton  
Location: Eastern Bass Strait  
Timeframe: completed 2012  
Investment: US$1.1 billion  
Status: Stage 1 of the Kipper project with capacities of 30 petajoules of gas and 10,000 barrels per day of oil condensate per year is being developed in eastern Bass Strait. When developed, gas and condensate from Kipper will be produced from four subsea wells and connected via a local subsea pipeline to the current offshore infrastructure for piping ashore to Longford. The Kipper gas project will be the first ever third-party-owned production to use the ExxonMobil operated Longford gas plant.

**TURRUM**

Participants: Esso Australia and BHP Billiton  
Location: Eastern Bass Strait  
Timeframe: Construction has commenced and the field is expected to commence producing in 2013.  
Investment: US$1.25 billion  
Status: The Turrum field holds approximately one trillion cubic feet of gas and 110 million barrels of oil and natural gas liquids. The project is based upon the construction of a new platform (Marlin B) bridge linked to the existing Marlin A platform in Bass Strait. The platform will process additional oil production and gas cycling which will be piped back to existing processing facilities at Longford.
WESTERN AUSTRALIA

Western Australia has approximately 120 trillion cubic feet of proved and probable reserves of natural gas. The ultimate recoverable gas resource may be in the order of 200 trillion cubic feet, according to the Western Australian Department of Industry and Resources. Western Australia is a significant producer of LNG for export and a supplier of natural gas for Western Australia industrial and domestic use. Approximately two thirds of Australia’s current natural gas production is from the Carnarvon Basin off the coast of Western Australia. Most of the gas currently produced in WA is transformed into LNG and exported to Japan.

New projects under development will see LNG production and export increase significantly with WA expected to provide approximately 60 million tonnes per annum of additional LNG capacity by 2020. More LNG projects are at the design stage and when developed will further strengthen WA as a major world LNG exporter.

Barrow, Thevenard and Varanus Island oil and gas plants feed the domestic gas pipelines and also produce oil for domestic use and for export. Offshore along the NWS and Timor Sea areas a number of fixed and floating oil production facilities produce oil and condensate for domestic use and export.

The country’s first LNG project, the North West Shelf Venture (NWSV), began shipping LNG in 1989. The project has since grown to include five production units (or trains) and it now produces up to 16.3 million tonnes per annum of LNG per year. The NWSV produces approximately two-thirds of Western Australian domestic gas requirements.

Western Australia has four major gas pipelines from the above gas production facilities supplying natural gas to the Perth, South West, Goldfields and Pilbara regions enabling mining and industrial development and gas fired electricity generation based on the reliable long term supply of gas energy.

North West Shelf LNG Joint Venture The NWS Gas Production Plant at Karratha has five trains producing 16.3 million tonnes per annum of LNG. The joint venture utilises 3 offshore platforms (North Rankin A, Goodwyn A and Angel) and the Cossack Pioneer FPSO to extract oil, gas and condensate from the North Rankin, Perseus, Hermes, Searipple and Lambert fields. To date over $27 billion has been invested in the project. More than 3000 LNG cargoes, more than 1260 condensate cargoes and more than 424 million barrels of oil have been delivered since 1989. North Rankin Redevelopment Project ($5 billion development) aims to recover any remaining low pressure gas from North Rankin and Perseus fields extending the field life to 2041. The Cossack Pioneer FPSO is being replaced by a new FPSO Okha which will have improved production capability.

Barrow and Thevenard Islands Barrow Island is located 50 kilometres off the Western Australia coast and 80 kilometres north of Onslow. Chevron has been producing oil on Barrow Island for 45 years. The Barrow Island oil fields are the largest onshore oil fields in Australia. Over 400 wells have been drilled across the southern half of the island producing oil and natural gas. Oil tankers are filled by a submarine pipeline that extends 10 km offshore to a tanker mooring buoy. Barrow Island is a Class A nature reserve. Thevenard Island is the hub from which crude oil from six offshore petroleum reservoirs – Saladin, Roller, Skate, Yammaderry, Cowle and Crest – is processed and readied for shipment by tankers. The Gorgon LNG Project will be sited on Barrow Island.
Varanus Island
Varanus Island, 75 kilometres offshore northwest Australia, is the hub for the Harriet Joint Venture and John Brookes Joint Venture oil, condensate and gas gathering infrastructure. Facilities include a fixed conventional oil platform at Harriet, monopod platforms at Victoria and Double Island, and the John Brookes platform; oil processing facilities and 750,000 barrels of liquid storage; five gas plants, two sales gas pipelines to the main West Australia’s gas trunklines and an oil export system.

Wandoo Field
Wandoo field is located approximately 80 kilometres north-west of the town of Karratha. The field consists of the Wandoo A Unmanned Monopod; Wandoo B Production Platform and a Single Point Tanker Mooring and Offloading Facility. Wandoo B is a concrete gravity structure connected to Wandoo A by an undersea pipeline. Oil is stored in the concrete structure supporting the Wandoo B processing facilities and then offloaded through flexible pipelines to a CALM Buoy located 1.2 kilometres north of the Wandoo B platform. A floating hose is used in transferring the oil from the CALM Buoy to export tankers situated at a mooring facility. Export tankers are chartered on a spot basis to offload the crude.

Enfield Oil Field
Enfield is located 50 kilometres north of Exmouth and uses 18 subsea wells to provide oil to a Floating Offshore Production and Storage (FPSO) vessel Nganhurra with a 100,000 bbl/d production capacity. Offload to oil tankers takes place via an astern floating hose from the FPSO to the receiving tanker.

Vincent Oil Field
Vincent is located 50km northwest of Exmouth with 13 subsea wells connected to the FPSO Maersk Ngujima, which has a 50,000 barrels per day production capacity.

Laminaria-Corallina Fields
The Laminaria and Corallina oil fields are located about 550 kilometres west-north-west of Darwin and 160 kilometres south of East Timor. The Laminaria and Corralina fields comprise five production wells and one gas injection well tied back to the FPSO, the Northern Endeavour, with a 180,000 barrels per day production capacity. The fields have produced around 195 million barrels of oil since 1999. Currently both fields produce about 10,000 barrels per day. The estimated field life of Laminaria-Corallina is to 2019.

Stybarrow Field
Stybarrow oil field is located 65 kilometres from Exmouth with 9 subsea wells supplying the FPSO Stybarrow Venture, which has a 80,000 barrels per day oil production capacity. At a water depth of approximately 825 metres Stybarrow is one of the deepest oil field developments undertaken in Australia to date. Stybarrow and the adjacent small oil rim of the Eskdale field have recoverable oil reserves estimated in a range of 60-90 million barrels of oil. Estimated economic life is to 2018.

Mutineer-Exeter oil fields
Mutineer-Exeter oil fields are located approximately 150km north of Dampier on the north-west coast of Australia, in the offshore Carnarvon Basin, Western Australia. The fields have 4 subsea wells supplying the FPSO MODEC Venture II with a 100,000 barrels per day oil production capability.

Van Gogh oil field
The Van Gogh field is 53 kilometres offshore from Exmouth and supplies oil to an FPSO, the Ningaloo Vision, which currently produces around 35,000 to 40,000 barrels of oil per day. The field has 19 production wells and production commenced in 2010.

Pyrenees oil field
The Pyrenees oil field is located in the Exmouth sub-basin. The project uses 13 wells tied to an FPSO, Pyrenees Venture, with a production capacity of approximately 96,000 barrels of oil and gas per day. Production commenced in 2010. The field contains an estimated 80 to 120 million barrels of recoverable oil and has a life of around 25 years.
**Woollybutt**  The Woollybutt Project in the Carnarvon Basin is operated by Eni (65 per cent interest) with joint venture partners Mobil Australian Resources Pty Ltd (Exxon Mobil) with a 20 per cent interest and Tap West Pty Ltd (Tap Oil), with a 15 per cent interest. The Woollybutt field was discovered in April 1997 in the well Woollybutt-1 and began production in 2003 through the FPSO facility, Four Vanguard. The southern lobe of the field was commissioned in mid 2009. To date the Woollybutt field has produced in excess of 32 million barrels of oil.

The following is a list of major oil and gas projects in Western Australia, including those under development or at project definition stage.

**In development**

**BROWSE LNG HUB**
- **Participants:** Woodside (Operator), Chevron, Royal Dutch Shell, BP and BHP Billiton
- **Location:** James Price Point area, north of Broome, Western Australia
- **Timeframe:** Final Investment Decision expected by mid 2012, 30 year Kimberley gas project
- **Investment:** $18.5 billion

**GORGON PROJECT**
- **Participants:** The Gorgon Project is operated by an Australian subsidiary of Chevron and is a joint venture of the Australian subsidiaries of Chevron (approximately 47 per cent), ExxonMobil (25 per cent) and Shell (25 per cent), Osaka Gas (1.25 per cent), Tokyo Gas (1 per cent) and Chubu Electric Power (0.417 per cent).
- **Location:** Barrow Island, Western Australia
- **Timeframe:** First LNG production is scheduled for 2014.
- **Investment:** $43 billion
- **Employment:** Peak construction employment in WA of around 10,000 direct and indirect jobs.
- **Status:** Approved, construction commenced in December 2009.

**MACEDON PROJECT**
- **Participants:** BHP Billiton Petroleum (Operator), Apache Corporation
- **Location:** NWS, Western Australia
- **Timeframe:** 2 years construction period from time of commencement
- **Investment:** US$1.5 billion
- **Status:** The Macedon Project includes the following components: four subsea wells, manifold, 20” subsea wet gas pipeline and umbilical to shore; Onshore Gas Plant for dehydration, dew pointing, water and condensate treatment and sales gas compression; Sales gas pipeline from Onshore Gas Plant to Dampier to Bunbury Natural Gas Pipeline tie-in; Onshore infrastructure including Construction Camp and Access Road to site. First production is expected during calendar year 2013.
NORTH RANKIN 2 REDEVELOPMENT
Participants: Woodside (Operator), BHP Billiton Petroleum, BP, Chevron, MIMI and Shell.
Location: NWS
Timeframe: Installation in 2010 with progressive start up in 2013.
Investment: $5 billion
Status: The project involves the construction and installation of a new platform (North Rankin B) and modification of the process modules of the existing platform. The new platform will be installed alongside the existing platform with a bridge linking the two.

PRELUDE FLNG
Operator: Shell
Location: Browse Basin, Western Australia
Timeframe: Detailed design and construction of the FLNG vessel is currently underway at the shipyard in South Korea. First production expected in 2017.
Investment: $15 to 20 billion
Status: Shell took final investment decision on the Prelude FLNG Project on 20 May, 2011. It will start building a FLNG to produce and export LNG off the coast of Australia at the site of the gas field.

WHEATSTONE PROJECT
Participants: Chevron (Operator – 73.6 per cent), Apache and KUFPEC
Location: Ashburton North, NWS, Western Australia
Timeframe: FID scheduled for the second half of 2011 with first gas production by end of 2016
Investment: $29 billion
Status: The project will consist of two train LNG processing plant, a separate domestic gas facility, LNG and condensate storage facilities, marine facilities including a shipping channel, turning basin, Materials Offloading Facility and export jetty, an accommodation village and other supporting infrastructure. Gas and condensate will be produced from the Wheatstone, Iago, Brunello and Julimar gas resources in the Carnarvon Basin.
DEVIL CREEK DEVELOPMENT PROJECT

Participants: Apache (Operator) has a 55 per cent interest in the Reindeer field and Devil Creek, with the remaining interest held by Santos (45 per cent).

Location: Reindeer Gas Field, NWS, Western Australia

Timeframe: The development is expected to have a life of 20 to 30 years and, having obtained all the necessary government approvals, project construction will commence in September 2009 and be in production by 2012.

Status: The Devil Creek Development Project comprises an unmanned offshore gas production platform in the Reindeer field off Dampier in the NWS, a 110 kilometres offshore gas supply pipeline and an onshore gas processing plant. The gas will be processed and then fed into the Dampier to Bunbury Natural Gas Pipeline. Devil Creek will be the third domestic gas hub in Western Australia after NWS and Varanus Island.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the Act</td>
<td>Inspector of Transport Security Act 2006</td>
</tr>
<tr>
<td>the Inspector</td>
<td>Inspector of Transport Security</td>
</tr>
<tr>
<td>the Minister</td>
<td>Minister for Infrastructure and Transport</td>
</tr>
<tr>
<td>ADF</td>
<td>Australian Defence Force</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AGCCC</td>
<td>Australian Government Crisis Coordination Centre</td>
</tr>
<tr>
<td>AIS</td>
<td>Automatic Identification System</td>
</tr>
<tr>
<td>AMIS</td>
<td>Australian Maritime Identification System</td>
</tr>
<tr>
<td>AMOSC</td>
<td>Australian Marine Oil Spill Centre</td>
</tr>
<tr>
<td>AMSA</td>
<td>Australian Maritime Safety Authority</td>
</tr>
<tr>
<td>AMSC</td>
<td>Area Maritime Security Committee (US)</td>
</tr>
<tr>
<td>API</td>
<td>American Petroleum Institute (US)</td>
</tr>
<tr>
<td>APPEA</td>
<td>Australian Petroleum Production and Exploration Association Ltd</td>
</tr>
<tr>
<td>AQTF</td>
<td>Australian Quality Training Framework</td>
</tr>
<tr>
<td>ARPA</td>
<td>Automatic Radar Plotting Aid</td>
</tr>
<tr>
<td>ASIC</td>
<td>Aviation Security Identification Card</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ATSA</td>
<td>Aviation Transport Security Act 2004</td>
</tr>
<tr>
<td>BLU</td>
<td>Business Liaison Unit (ASIO)</td>
</tr>
<tr>
<td>BOEM</td>
<td>Bureau of Ocean Energy Management (US)</td>
</tr>
<tr>
<td>BOEMRE</td>
<td>Bureau of Ocean Energy Management, Regulation and Enforcement (US)</td>
</tr>
<tr>
<td>BOSIET</td>
<td>Basic Offshore Safety Induction and Emergency Training (UK)</td>
</tr>
<tr>
<td>BPC</td>
<td>Border Protection Command</td>
</tr>
<tr>
<td>BSEE</td>
<td>Bureau of Safety and Environmental Enforcement (US)</td>
</tr>
<tr>
<td>CBP</td>
<td>Customs and Border Protection (US)</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team (AUSTRALIA)</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CMATS Treaty</td>
<td>Treaty on Certain Maritime Arrangements in the Timor Sea</td>
</tr>
<tr>
<td>CPA</td>
<td>Closest Point of Approach</td>
</tr>
<tr>
<td>CPNI</td>
<td>Centre for the Protection of National Security (UK)</td>
</tr>
<tr>
<td>CPP</td>
<td>Certified Protection Professional (US)</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSG</td>
<td>Coal Seam Gas</td>
</tr>
<tr>
<td>CSOC</td>
<td>Cyber Security Operations Centre</td>
</tr>
<tr>
<td>DECC</td>
<td>Department of Energy and Climate Change (UK)</td>
</tr>
<tr>
<td>DIDO</td>
<td>Drive-In, Drive Out</td>
</tr>
<tr>
<td>DNC</td>
<td>Digital Nautical Charts</td>
</tr>
<tr>
<td>DOS</td>
<td>Declaration Of Security</td>
</tr>
<tr>
<td>DPI</td>
<td>Department of Primary Industries (Victoria)</td>
</tr>
<tr>
<td>DRET</td>
<td>Department of Resources Energy and Tourism</td>
</tr>
<tr>
<td>DSC</td>
<td>Digital Selective Calling</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECDIS</td>
<td>Electronic Chart Display and Information System</td>
</tr>
<tr>
<td>EEZ</td>
<td>Exclusive Economic Zone</td>
</tr>
<tr>
<td>ENC</td>
<td>Electronic Navigational Charts</td>
</tr>
<tr>
<td>EPOL</td>
<td>Emergency Preparedness Offshore Liaison Group</td>
</tr>
<tr>
<td>ESG</td>
<td>Energy Security Group</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation (US)</td>
</tr>
<tr>
<td>FIFO</td>
<td>Fly-In, Fly-Out</td>
</tr>
<tr>
<td>FLNG</td>
<td>Floating LNG</td>
</tr>
<tr>
<td>FPSO</td>
<td>Floating Production, Storage and Offtake Unit</td>
</tr>
<tr>
<td>FSU</td>
<td>Floating Storage Unit</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office (US)</td>
</tr>
<tr>
<td>GMDSS</td>
<td>Global Maritime Distress and Safety System</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GRN</td>
<td>Global Response Network</td>
</tr>
<tr>
<td>GV-ID</td>
<td>Globally Verifiable Identity</td>
</tr>
<tr>
<td>HSE</td>
<td>Health and Safety Executive (UK)</td>
</tr>
<tr>
<td>IALA</td>
<td>International Association of Marine Aids to Navigation and Lighthouse Authorities</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organisation</td>
</tr>
<tr>
<td>ISPS Code</td>
<td>International Ship and Port Facility Security Code</td>
</tr>
<tr>
<td>JPDA</td>
<td>Joint Petroleum Development Area</td>
</tr>
<tr>
<td>LNG</td>
<td>Liquefied Natural Gas</td>
</tr>
<tr>
<td>LOOP</td>
<td>Louisiana Offshore Oil Port (US)</td>
</tr>
<tr>
<td>LPG</td>
<td>Liquefied Petroleum Gas</td>
</tr>
<tr>
<td>LRAD</td>
<td>Long Range Acoustic Device</td>
</tr>
<tr>
<td>LRIT</td>
<td>Long Range Identification and Tracking</td>
</tr>
<tr>
<td>MARSEC</td>
<td>Maritime Security Level</td>
</tr>
<tr>
<td>MCA</td>
<td>Maritime and Coastguard Agency (UK)</td>
</tr>
<tr>
<td>MODU</td>
<td>Mobile Offshore Drilling Unit</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MSG</td>
<td>Maritime Security Guard</td>
</tr>
<tr>
<td>MSIC</td>
<td>Maritime Security Identification Card</td>
</tr>
<tr>
<td>MSRAM</td>
<td>Maritime Security Risk Analysis Model</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>MTSA</td>
<td>Maritime Transport Security Act 2003</td>
</tr>
<tr>
<td>MWCC</td>
<td>Marine Well Containment Company (US)</td>
</tr>
<tr>
<td>NALECC</td>
<td>National Law Enforcement Coordinating Committee, Philippines</td>
</tr>
<tr>
<td>NCTC</td>
<td>National Counter Terrorism Committee</td>
</tr>
<tr>
<td>NMIC</td>
<td>National Maritime Information Centre (UK)</td>
</tr>
<tr>
<td>NOPSA</td>
<td>National Offshore Petroleum Safety Authority</td>
</tr>
<tr>
<td>NOPSEMA</td>
<td>National Offshore Petroleum Safety and Environmental Management Authority</td>
</tr>
<tr>
<td>NPD</td>
<td>Norwegian Petroleum Directorate</td>
</tr>
<tr>
<td>NWS</td>
<td>North West Shelf (off the coast of Australia)</td>
</tr>
<tr>
<td>NWSV</td>
<td>North West Shelf Venture</td>
</tr>
<tr>
<td>OCS</td>
<td>Outer Continental Shelf</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Cooperation and Development</td>
</tr>
<tr>
<td>OGSF</td>
<td>Oil and Gas Security Forum</td>
</tr>
<tr>
<td>OGP</td>
<td>International Association of Oil and Gas Producers</td>
</tr>
<tr>
<td>OLF</td>
<td>Norwegian Oil Industry Association</td>
</tr>
<tr>
<td>OSAC</td>
<td>Overseas Security Advisory Council (US)</td>
</tr>
<tr>
<td>OTS</td>
<td>Office of Transport Security</td>
</tr>
<tr>
<td>PCI</td>
<td>Professional Certified Investigator (US)</td>
</tr>
<tr>
<td>PISAS</td>
<td>Petroleum Industry Security Alert System</td>
</tr>
<tr>
<td>PJCLE</td>
<td>Parliamentary Joint Committee on Law Enforcement</td>
</tr>
<tr>
<td>PLO</td>
<td>Police Liaison Officer</td>
</tr>
<tr>
<td>PQS</td>
<td>Personal Qualification Standard</td>
</tr>
<tr>
<td>PSA</td>
<td>Petroleum Safety Authority Norway</td>
</tr>
<tr>
<td>PSP</td>
<td>Physical Security Professional</td>
</tr>
<tr>
<td>RPT</td>
<td>Regular Passenger Transport</td>
</tr>
<tr>
<td>SAR</td>
<td>Search and Rescue</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>SIEVS</td>
<td>Suspected Illegal Entry Vessels</td>
</tr>
<tr>
<td>SOLAS</td>
<td>Safety of Life at Sea Convention 1974</td>
</tr>
<tr>
<td>SOSREP</td>
<td>State of Service Representative for Maritime Salvage and Intervention (UK)</td>
</tr>
<tr>
<td>TCPA</td>
<td>Time to Closest Point of Approach</td>
</tr>
<tr>
<td>Timor Sea Treaty</td>
<td>Timor Sea Treaty between the government of East Timor and the government of Australia, 2002</td>
</tr>
<tr>
<td>TISN</td>
<td>Trusted Information Sharing Network</td>
</tr>
<tr>
<td>TWIC</td>
<td>Transport Worker Identification Credential (US)</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>USCG</td>
<td>United States Coast Guard</td>
</tr>
<tr>
<td>VLCCs</td>
<td>Very Large Crude Carriers</td>
</tr>
<tr>
<td>VTS</td>
<td>Vessel Traffic Service</td>
</tr>
</tbody>
</table>
References

39. Economic data and statistics contained in the Australian Oil and Gas Operations Section was provided by the Australian Petroleum Production and Exploration Association (APPEA) and the Bureau of Resource and Energy Economics.

40. Government of Western Australia, Department of Mines and Petroleum, Major Resources Projects, Western Australia 2012, 2012


54. RAN Australian Hydrographic Service, chart extract developed for the Inquiry


59. RAN Australian Hydrographic Service, chart extract developed for the Inquiry


62. Information contained in the cyber security chapter was obtained primarily from information provided at the SMi – Oil and Gas Cyber Security Forum 2011, Securing the Oil & Gas Industry from Future Cyber Threats, 21-22 November 2011, London, UK
