CHAPTER THREE

TELECOMMUNICATIONS SECURITY SECTOR REFORM

1. Introduction

Australia's national security, economic prosperity and social wellbeing is increasingly reliant on the Internet and other information and communications technologies (ICT). Underpinning our use of these technologies is our telecommunications infrastructure. However, there are very real challenges to ensuring its security in the face of criminal and strategic threats. Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental mis-configuration, external hacking and even trusted insiders. As customers, Australian citizens, businesses and public entities rely on public telecommunication carriers and carriage service providers (C/CSPs) to handle their data and personal information securely. The security of C/CSPs' networks is, however often opaque to customers who are usually unaware of breaches. Failure to manage the security risks has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.

The Australian Government is considering whether telecommunications legislation, such as the *Telecommunications Act (1997)* (Telecommunications Act) and other relevant legislation should be amended to establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure. PJCIS views on the proposed Telecommunications Sector Security Reform (TSSR) are expressly sought by Government to assist it in deliberations about measures to take forward.

The desired outcomes of the proposed framework are that:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities, and
- the privacy of customer information is better assured.

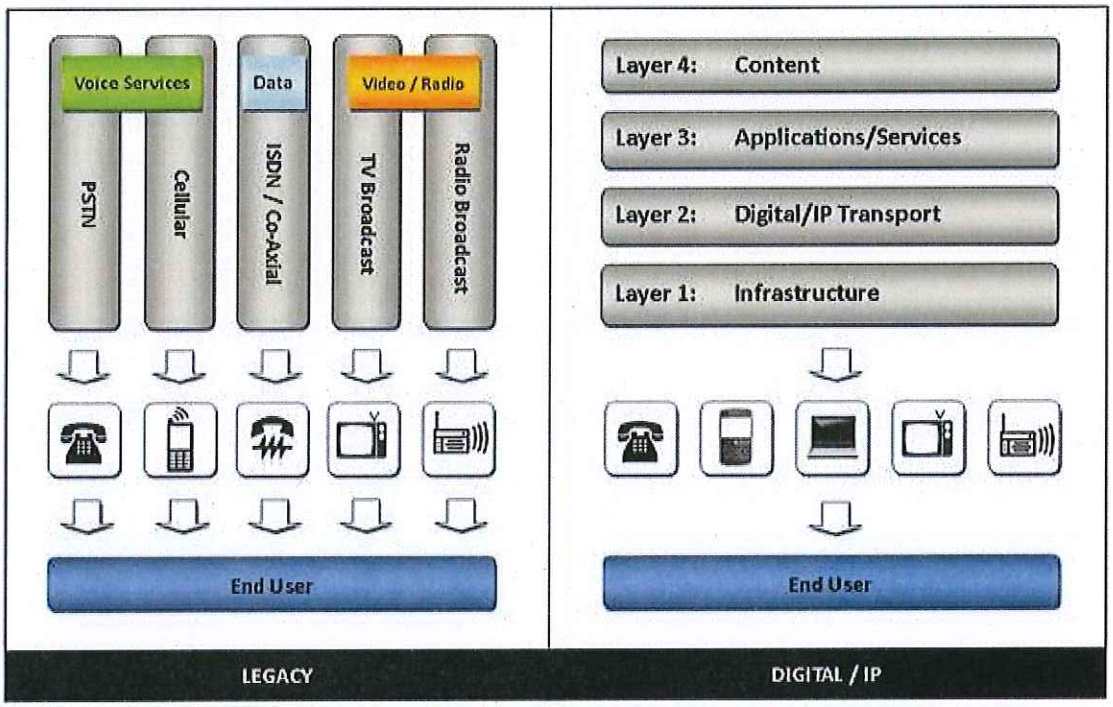
2. The context

While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment.

2.1 Australia's telecommunications industry

Australia's telecommunications industry consists of a wide range of services and participants — an increasing number of which are based outside Australia. The telecommunications industry is a highly dynamic one, and C/CSPs usually operate network environments that have been significantly expanded and modified from their original specifications. In a broad sense, global telecommunications network architecture has evolved over the past 30 years from a 'siloed' services model to one of 'layered' convergence (figure 1) . In Australia today, our telecommunications industry has evolved to reflect this shift, while the standardisation and mass-production of network equipment has also cut costs and opened up the range of suppliers with new entrants to the market gaining a stronger presence.

Figure 1: Convergence in network and service layers[28]



The National Broadband Network (NBN) rollout will transform Australian telecommunications infrastructure. This will result in further changes to the telecommunications retail market's structure and functionality, including creating new opportunities for market participation. Australia's telecommunications industry is increasingly diverse, with a range of overlapping and interconnected platforms and networks. The provision and operation of software platforms within networks has also emerged as a separate activity. These systems include such things as content distribution networks to optimise the delivery of content, and other operational and business support systems, including those that utilise, update and store customer information. The evolution of over-the-top (OTT) service providers (e.g. Google and Yahoo, eBay, Facebook and iTunes) has also been quite significant. Many of these service providers are global and more likely to form partnerships with local content providers (eg ninemsn and Yahoo!7) than vertically integrate with domestically-owned networks.

The Australian Government recognises that C/CSPs operate in an increasingly competitive, commercial environment and that security is only one factor in procurement and

[28] Australian Communications and Media Authority, 2011, Broken Concepts: The Australian Communications legislative landscape, p6 http://engage.acma.gov.au/wp-content/uploads/2011/08/ACMA_Broken-Concepts_Final_29Aug1.pdf

investment decision-making. Although there are market incentives and customer expectations for network providers to ensure their infrastructure and services are secure, C/CSPs are working with incomplete information about the national security environment. There will always be information available to Government which is beyond industry's reach. In many cases C/CSPs provide packaged services as a subscription. Customers have the power to choose from the packages on offer, but do not have the leverage to demand tailored services or require higher levels of transparency or security. This lack of awareness, combined with the technical complexity, mean that most customers lack the ability to negotiate the security configuration they want their C/CSP to provide. Rather, customers are only able to specify the security outcome they want achieved. The effects of inadequate security by C/CSPs are potentially much greater on customers than on the carrier itself. And yet it is the C/CSP that decides a fundamental part of ICT security for most Australians.

2.2 National security risks

The *ASIO Report to Parliament 2010-2011* states that espionage by foreign intelligence services is an enduring security threat to Australia, both conventional and new forms, such as cyber espionage. Our increasing reliance on communications technology to conduct the business of Government, commerce and our daily lives makes Australians more vulnerable to malicious attack. As such cyber security has emerged as a serious and widespread concern. [29] States, as well as disaffected individuals or groups, are able to use computer networks to view or siphon sensitive, private, or classified information for the purpose of, political, diplomatic or commercial advantage.

Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available. This threat extends to information vital to the effective day-to-day operation of critical national industries and infrastructure, including intellectual property and commercial intelligence.[30]

2.3 Current telecommunications regulatory environment

Australia's telecommunication industry is regulated primarily under two pieces of legislation — the *Telecommunications Act (1997)* administered by the Minister for Broadband, Communications and the Digital Economy and the *Telecommunications (Interception and Access) Act (1979)* (TIA Act) administered by the Attorney-General.

[29] ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011

[30] ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011

Section 581 of the Telecommunications Act provides the Attorney-General (in consultation with the Prime Minister and the Minister for Broadband, Communications and the Digital Economy) the power to give written direction to C/CSPs to cease supply of a carriage service if the use of that service is or would be prejudicial to security. It is recognised that such action, would impact on both businesses and consumers. Section 581 is non-specific, is not triggered by a specific set of circumstances and does not allow a practical graduated response to security risks. This sanction is a blunt instrument, which is not working to provide disincentives for C/CSPs to ignore national security risks when making business decisions about the design of their networks.

Under section 202B of the TIA Act, C/CSPs are obliged to notify Government of planned changes to a telecommunications service or system where these changes may affect their capacity to comply with their obligations under the TIA Act. The TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure.

2.4 Analysis

Engagement between Government and the telecommunications industry about national security risks currently occurs on an informal basis, relying on co-operation between security agencies and C/CSPs in cases where security agencies become aware of potential risks. In most cases engagement between security agencies and C/CSPs has been constructive. However there is a lack of awareness of national security risks in business decisions by many C/CSPs, which means engagement often occurs late in the decision making process. A more defined framework for government's engagement with industry would minimise disruption and resource impacts for industry and government. It would also provide greater clarity for industry during a time of considerable structural change in the telecommunications industry.

Based on the information available to it, Government considers that the market is inadequately responding to issues of national security. As both businesses and consumers are also exposed to the consequences of potential security risks, there is a compelling case to act now. The telecommunications market's current commercial incentives do not compel the industry to address national security issues. Australia is at a critical stage of telecommunications infrastructure development driven by the NBN's construction. Delaying action to make C/CSPs aware of managing national security risks will complicate long term management decisions made on the design and procurement of major telecommunications infrastructure, with potential negative impacts on national security.

Accordingly, Government has a responsibility to intervene in the market to educate and assist C/CSPs to maintain a minimum level of security for the purpose of protecting the data

on their networks and, ultimately to ensure mechanisms are in place to support the integrity and security of Australia's national telecommunications infrastructure.

3. Proposed approach

One approach to address national security risks relating to telecommunications infrastructure may be achieved using a regulatory framework. Such an approach was developed earlier in 2012 for consultation with industry.

A regulatory approach could be achieved by making amendments to the Telecommunications Act, and other relevant legislation, such that C/CSPs protect their networks from unauthorised interference with the following elements:

1. an industry-wide obligation on all C/CSPs to protect their infrastructure, customer owned data and information about customers from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;
2. a requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and
3. powers of direction and a penalty regime to encourage compliance.

In designing a regulatory framework, the following principles are considered important elements of an effective regulatory system:

- be adaptable to a changing environment;
- be clear to industry;
- provide incentives for compliance;
- be reasonably equitable; and
- not be resource-intensive for industry to comply or for government to administer.

The advantages of such a framework include that it could:

- focus on security outcomes rather than absolute technical requirements, making it adaptable to changes in technology and the telecommunications market,
- provide greater clarity, control and certainty for industry by focusing on self-governance and demonstration of compliance,
- can be applied equitably across the telecommunications sector, and

- provides a more effective incentive for industry to place greater emphasis on national security considerations in its business decisions.

The Government is aware that such a framework may have significant impacts for industry and agencies and welcomes input as it explores how such an approach could work in practice and what these impacts may be.

It should be noted that some classified national security information will only be able to be shared with companies that have entered into security agreements with Government, which have been negotiated on the basis of risk to the national interest.

3.1 Industry consultation

Targeted consultation with industry occurred in early 2012, during which C/CSPs demonstrated an understanding of the importance of protecting the confidentiality, integrity and availability of their networks.

Other points raised by industry included:

- the desire for a level playing field across the industry,
- a desire for clear guidance about Government's expectations and requirements for industry compliance,
- the need for certainty to enable C/CSPs to undertake business decisions with confidence, and
- flexibility for industry to explore and experiment with efficient and effective solutions for managing security risks.

During the consultation about a possible regulatory framework that originally included a notification obligation in place of the requirement to provide information to Government on request, industry expressed a preference for an approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it. As a consequence the Government has been considering alternative ways that a regulatory framework may be designed with less focus on administrative processes and technical requirements, but greater emphasis on outcomes.

3.2 Compliance framework

C/CSPs are obliged to protect the privacy of their customers' information; however there are many different ways that a C/CSP may be organised which will affect its ability to be able to confirm the security of its network and the information held on it. Where a C/CSP relies heavily on sub-contracted, or outsourced or off-shored maintenance or services it will be

more complicated to oversee the maintenance of security than a C/CSP that manages its network and information held on it in-house.

The industry consultation has led Government to consider whether a compliance framework, based on requiring C/CSPs to be able to demonstrate competent supervision and effective controls over their networks, may be a more effective approach. Such an approach would focus on the ability of a C/CSP to manage the security of its infrastructure and customer owned data and information about customers. Information about a possible 'compliance framework' is provided below.

Competent supervision refers to the ability of a C/CSP to maintain technically proficient oversight (either in-house or through a trusted third party) of the operations of their network, and the location of data; awareness of, and authority over, parties with access to network infrastructure ;and a reasonable ability to detect security breaches or compromises.

Effective control refers to the ability of a C/CSP to maintain direct authority and / or contractual arrangements which ensure that its infrastructure, customer owned data and information about customers is protected from unauthorised interference (which refers to network access). This would include arrangements to:

- cease contracts where there has been a security breach,
- direct contractors to carry out mitigation or remedial actions,
- oblige contractors to monitor and report breaches to the C/CSP, and
- repatriate customer data and network systems where unauthorised interference to a network has occurred.

Under such a compliance framework, Government would provide guidance to assist industry to understand and meet its obligation, and to inform C/CSPs how they can maintain competent supervision and effective control over their networks. Guidance would be tailored to C/CSP service types (for example internet service providers (ISP), cloud computing providers, and mobile virtual network operators) and distributed to C/CSPs prior to commencement of a framework.

Government's aim under a regulatory framework would be to promote risk informed management of security in the telecommunications sector. This could be achieved by educating C/CSPs on national security risks and encouraging ongoing awareness and responsibility for network security, reducing the need for Government intervention. Provision of general security advice, briefings and the development of guidance would be

intended to be an ongoing, iterative process conducted in cooperation with industry, which would reflect evolving technologies and markets.

Under a regulatory framework Government would also disseminate information on specific security threats to affected C/CSPs on an as needs basis, including:

- targeted briefings (specific threat and risk information), and
- provision of specific mitigation information.

In order to monitor compliance with the obligations under a framework C/CSPs would be required upon request, to demonstrate compliance to Government. . This could be done by compliance assessments and audits, based on a risk assessment to inform the level of engagement required. The level of engagement would be informed by factors such as:

- market share
- customer base, and
- service offerings.

Government is giving consideration to the means by which it could be assured that industry had taken reasonable mitigations steps to address security risks. It would benefit from the Committee's advice on appropriate assurances mechanisms. These might include accreditation of industry for self-assessment purposes or a role for third parties in providing audit and assurance services. For example, more in depth compliance assessment and audit could focus on C/CSPs that security agencies consider are at greater risk of national security threats. Less intensive compliance assessment and audits would apply to selected C/CSPs from the broader pool of lower risk entities. This approach would monitor and evaluate industry-wide C/CSP governance arrangements to ensure competent supervision and effective control over their networks and facilities.

3.3 Directions and penalties

Government would seek to use advice and guidance to encourage risk informed management of security concerns. Where potential issues of concern are identified, Government's preferred approach would be to engage with the relevant C/CSP to establish whether the concerns can be co-operatively addressed. Where this is not possible, one way to proportionately address various levels and forms of non-compliance could be to provide a graduated suite of enforcement measures (including the power of direction). The availability of enforcement measures would provide industry with greater incentive to engage co-operatively.

Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government's confidence in

the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. To safeguard such a power, it could require the Secretary of the Attorney General's Department, to seek the concurrence of the Director General of Security and the Secretary of the Department of Broadband, Communications and the Digital Economy, before directing a C/CSP to alter its business practices or undertake other actions considered necessary to protect national security interests. This would generally follow a period of more direct and intensive engagement with the C/CSP concerned.

Directions could involve targeted mitigation or remediation of security risks including modifications to infrastructure, audit, and ongoing monitoring, with costs to be borne by the relevant C/CSP. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters.

To encourage C/CSPs' recognition and compliance with their security obligations under this regulatory framework, financial penalties are proposed. Financial penalties would be used in situations where, for example a C/CSP fails to take reasonable action to protect its infrastructure, customer owned data or information about customers. These penalties would be modelled on existing civil penalties contained in the Telecommunications Act.

As described earlier, the current provision under subsection 581(3) of the Telecommunications Act would remain available for the most serious security breaches. This enables the Attorney-General, in consultation with the Prime Minister and Minister for Broadband, Communications and the Digital Economy, to direct C/CSPs to not use or supply, or cease using or supplying, particular services where such use or supply would be prejudicial to security. As this direction only applies to a service as a whole, however; it cannot be used to restrict service use or supply to a particular organisation, group or person. As such, subsection 581(3) is considered an option of last resort, applicable in very limited circumstances.

Should a graduated suite of enforcement measures be made available under a regulatory framework, the following circumstances provide an illustration of where the Government may consider taking enforcement action::

- **where a breach has occurred**, for example a CSP's data is accessed and published, demonstrating a failure to protect its infrastructure, customer owned data and information about customers from unauthorised interference,
- **where a C/CSP fails to provide reasonable assistance to Government to demonstrate compliance, if requested,**

- **where there is failure by a C/CSP** to undertake mitigation activities that Government has determined are necessary to protect its infrastructure, customer owned data and information about customers from unauthorised interference,
- **where there is failure by a C/CSP to otherwise satisfactorily demonstrate it has competent supervision or effective control.**

The framework is intended to maximise cooperative engagement between C/CSPs and Government on matters of national security. Where this relationship works effectively, there may be no need to invoke more formal directive powers. Administrative penalties or directions to C/CSPs would only be imposed where a risk has been assessed as significant and prior engagement has proved ineffective.

3.4 Transition arrangements

Should any legislative changes be agreed, this would require all C/CSPs to comply with the security obligations. In some instances this will require the application of mitigation measures to existing infrastructure. The security obligations would apply to existing infrastructure, new infrastructure as well as those being ordered. Government recognises that it would need to work closely with industry to ensure that there is a reasonable transition period.

4. Next Steps

Government recognises that a regulatory framework will include a cost to industry, and it is working to understand these costs through targeted consultation. This work will be complemented by the Parliamentary Joint Committee on Intelligence and Security's consideration.

CHAPTER FOUR

AUSTRALIAN INTELLIGENCE COMMUNITY LEGISLATION REFORM

1. Introduction

It is the responsibility of Government to protect society against threats to our national security. The Government must be vigilant and take appropriate action to ensure that any threats to our national security do not materialise. Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats.

However, the security environment is continually evolving and becoming increasingly diversified. Security legislation, and the ability of intelligence agencies to protect the security and safety of Australians and our democratic institutions, must also adapt and keep pace with these changes. To enable Australia's intelligence agencies to continue to protect national security, it is imperative that these agencies are appropriately equipped with the necessary statutory powers to uphold Australia's vital national security interests.

The Attorney-General's Department and Australian Intelligence Community agencies — including the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and the Defence Imagery and Geospatial Organisation (DIGO)—have identified a number of practical difficulties with the legislation governing the operation of these agencies, specifically the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

Addressing the problems outlined in this chapter of the Discussion Paper is necessary to maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.

At the same time, it is important that legislation governing intelligence agencies continues to include appropriate checks and balances on the exercise of their powers. Ensuring these agencies remain accountable for their actions helps to maintain public confidence in and support for the crucial work of intelligence agencies. The proposed reforms seek to maintain a strong and accountable legislative regime under which intelligence agencies can respond effectively when threats to our community emerge.

This chapter of the Discussion Paper outlines the problems identified in the operation of both the ASIO and IS Acts and contains three sections relating to matters the Government wishes to progress, matters the Government is considering, and matters on which the Government expressly seeks the views of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

2. Matters the Government wishes to progress

2.1 Modernise and streamline ASIO's warrant provisions

Division 2 of Part III of the ASIO Act contains a range of powers that ASIO can use under warrant in carrying out its statutory functions. The powers include search warrants, computer access warrants, listening and tracking device warrants, and the power to inspect postal or delivery service articles. Although there have been several amendments to each of these powers in the past, the amendments have been piecemeal and have not kept pace with technological advancements. To maintain effective intelligence gathering techniques and capabilities, these powers require modernising to provide a statutory framework which facilitates intelligence collection by the most technologically effective and efficient means.

References to 'computer' in section 25A

Computer access warrants under section 25A of the ASIO Act are limited to data stored on '*a computer*' ('computer' is defined to mean a computer, a computer system or part of a computer system). Therefore, if an individual has more than one computer which is not part of the same computer system, or data is stored on a computer network, more than one warrant may be necessary. For example, if there are multiple computers on a premises, and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, it would be necessary to seek another warrant (and enter the premises a second time) to access the data on that particular computer. This is inefficient and does not increase the level of accountability around the issue of warrants.

A possible solution to this issue could be to amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.

Variation of a warrant

Currently, the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in circumstances. A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability.

Duration of warrants

All warrants under the ASIO Act currently last for a maximum of six months, except for a search warrant which must be executed within 90 days. A warrant enabling a search to take place within a six month period would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors. Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required. .

To address this, the maximum duration of a search warrant could be increased from 90 days to six months, making it consistent with the other warrant powers in the ASIO Act.

Renewal of warrants

Certain threats to security can endure for many years, requiring a significant proportion of warrants issued under the ASIO Act to continue beyond the initial authorisation period. However, the current provisions in the ASIO Act do not enable a warrant to be extended.

In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources.

2.2 Modernise the ASIO Act employment provisions

Part V of the ASIO Act provides for the employment of ASIO officers and employees. These provisions do not align with the Australian Public Service (APS) framework as they were largely drafted over 30 years ago. Specific examples are discussed below.

Requirement to hold an "office"

Section 85 of the ASIO Act provides that the Director-General may determine the designation of officers in ASIO. Under subsection 85(1) of the ASIO Act, an officer must hold an 'office' that has been designated by the Director-General. With the exception of the Director-General, ASIO employees are no longer employed under the concept of the designation of 'office'. In practice, ASIO employees are employed under a concept of level. As it is no longer relevant, this section could be considered for deletion from the ASIO Act.

Descriptors of employment in the ASIO Act

The ASIO Act uses several descriptors to denote a person as an 'employee' of ASIO. These descriptors include 'officer,' 'employee' and 'staff' and are not separately defined in the ASIO Act. The use of the separate terms reflects the various amendments made to the ASIO

Act since 1979 but causes confusion as to whether differences between the terms are intended.

The use of the single term 'employee' throughout the ASIO Act would clarify and ensure consistency in the Act.

Special provisions relating to ASIO employees

Section 87 of the ASIO Act provides that the terms and conditions, under which ASIO employees were employed immediately before the date of commencement of the ASIO Act, continue to apply until they are varied by agreement. There are no longer any ASIO employees affected by section 87 and it could be considered for deletion from the Act.

Modernise the Director-General's powers in relation to employment terms and conditions

The Director-General's powers and responsibilities could be modernised so they are similar to those given to the CEO of a Commonwealth department or agency under the Public Service Act. This would ensure that, subject to guidelines issued by the Attorney under paragraph 8A(1)(b) of the ASIO Act, the Director-General has the power to engage employees on behalf of the Commonwealth, the rights, duties and powers of an employer and may determine terms and conditions of employment.

Proposed secondment arrangements

In order to access specialist skills and as part of arrangements whereby ASIO works closely with other agencies, ASIO often places staff of other agencies to work within ASIO, or agrees to its staff members working in other agencies. Legal complexities can arise in making such arrangements because of the specified scope of the functions and powers of ASIO and the other organisation involved.

If the ASIO Act were amended to expressly enable staff to be 'seconded' to and from ASIO and to clarify that, during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation, it would enhance ASIO's ability to engage with other agencies, and overcome administrative difficulties ASIO currently experiences in relation to existing secondment arrangements.

Such a secondment regime would operate independently from section 19A of the ASIO Act and section 13A of the IS Act. Section 19A enables ASIO to cooperate with and assist intelligence agencies, law enforcement agencies and prescribed Commonwealth and State authorities. An ASIO officer working in a multi agency task force operating under section 19A continues to carry out the functions of ASIO. Those functions would (as a consequence

of section 19A) include carrying out the functions of the other agencies involved in the task force. It is suggested that, unlike section 19A arrangements, these secondment arrangements would not be limited to intelligence, law enforcement and prescribed agencies.

2.3 Clarify the authority of the Defence Imagery and Geospatial Organisation

Minor amendments to DIGO's function under section 6B(e) of the IS Act would make some minor clarifications to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions.

At present the IS Act enables DIGO under its subsection 6B(e) function to:

a. provide imagery and geospatial data to produce non-intelligence products for use by Commonwealth, State and Territory authorities, as well as for certain non government bodies and foreign governments approved by the Minister (paragraph 6B(e)(i))

b. provide technical assistance to the Australian Defence Force, Commonwealth, State and Territory agencies (as well as to certain approved non-government bodies and foreign governments approved by the Minister) in relation to the production and use of imagery and geospatial products, not being 'intelligence information' obtained for the purposes of subsections 6B(a), (b) or (c) (para. 6B(e)(ii)), and

c. provide assistance in relation to Commonwealth, State and Territory authorities (as well as for certain non-government bodies and foreign governments approved by the Minister) in relation to the performance of these authorities or bodies of emergency response functions (as defined by the IS Act).

DIGO's work under this function may therefore involve collecting imagery and other data in relation to locations inside and outside Australia, but what distinguishes its subsection 6B(e) function from DIGO's 'intelligence functions' under subsections 6B(a) to (d), is that the work is not done for the purpose of providing information about a particular person or entity. This does not mean that intelligence sources or capability are not utilised for the function, but rather DIGO's intent, or the activities which are undertaken for the purposes of this function, do not fall within the scope of 'intelligence information' purposes (as defined by the IS Act.)

It is proposed that, amending paragraph 6B(e)(ii) of the IS Act would clarify the activities that are included in the scope of this function. These amendments would seek to:

a. Clarify the scope of application of paragraph 6B(e)(ii) - The current wording of paragraph 6B(e)(ii) is; 'assistance in relation to the use of such imagery and products'. The inclusion of the word 'such' in this subsection has given rise to an unintended encumbrance, as it has the effect of linking this function to the preceding paragraph 6B(e)(i) function. The original intent of paragraph 6B(e)(ii) was to enable DIGO to provide expert technical assistance and advice on the production and use of all DIGO imagery and geospatial products, not only with respect to its 'non-intelligence information' activities and products covered by paragraph 6B(e)(i).

Paragraph 6B(e)(ii) could be amended to remove the word 'such', so as to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.

b. Include an express reference to specialised imagery and geospatial technologies - DIGO has an express function under paragraph 6B(e)(ii) to provide assistance in relation to the production and use of imagery and other geospatial products to Commonwealth, State and Territory authorities and bodies approved in writing by the Minister.

In line with this function (and implied under DIGO's 'communication' function in subsection 6B(d) for the purposes of subsections 6B(a) to (d)), DIGO assists Commonwealth, State and Territory authorities (as well certain non-government bodies and foreign governments as approved by the Minister) with the use and application of specialised imagery and geospatial technologies, including geospatial web-based services. However, this is not expressly provided for as a function of DIGO.

An express reference to this activity would avoid any doubt that DIGO is able to assist in this way and to ensure the prevention of any perceived gaps in DIGO's functions. These changes would further provide DIGO with the scope and flexibility to meet White Paper objectives, including the proposed acquisition of domestic satellite collection capability by Defence.

The proposed amendments do not change the original intended operation of section 6B of the IS Act. The existing safeguards in the IS Act would remain unaffected and in place. The suggested changes involve minor clarifications to provide more certainty and practical utility. By making the legislation clearer, it would be easier for the Inspector-General of Intelligence and Security to effectively review whether DIGO is operating within its powers, and ensure accountability is maintained.

3. Matters the Government is considering

3.1 Amend the ASIO Act to create an authorised intelligence operations scheme

ASIO's continued ability to collect useful and relevant intelligence on the most serious threats to the security of Australia and Australians, hinges on its capacity to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability, in the course of their work.

With the enactment of broad overarching laws criminalising security related issues, many of those targets under investigation are involved in activities that breach the criminal law. Increasingly, those laws are capable of capturing the activities of persons who are associating covertly with targets, notwithstanding that their activities are for lawful intelligence collection purposes.

For example, under Part 5.3 of the Criminal Code, it is an offence to intentionally provide training to or receive training from a terrorist organisation where the person is reckless as to whether the organisation is a terrorist organisation. Therefore, if an ASIO officer or human source is tasked to collect covert intelligence in relation to a terrorist organisation, they may be open to criminal liability under the Criminal Code if, in the course of collecting the relevant intelligence, they receive training from that organisation.

An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens. A scheme similar to the controlled operations scheme under the *Crimes Act 1914* could be developed to apply to ASIO officers and human sources operating under the ASIO Act, with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations.

Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include:

- the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months)

- oversight and inspection by the Inspector-General of Intelligence and Security (IGIS), including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General
- specifying conduct which cannot be authorised (eg, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and
- independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.

3.2 Modernise and streamline ASIO's warrant provisions

Named person warrants

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.

Surveillance Devices – use of optical devices

Legislation governing ASIO's capabilities with respect to electronic surveillance has not been updated to align with legislation governing the use of electronic surveillance by law enforcement. ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement.

In practice, this acts as an impediment to effective cooperation and collaboration with law enforcement partner agencies. For example, the differences in scope and terminology between the ASIO Act and the Surveillance Devices Act limit actions which can be taken by each agency in working with partner agencies. Aligning the surveillance device provisions in the ASIO Act with the more modern Surveillance Devices Act could assist in overcoming these impediments to cooperation.

Authority for acts necessary to execute a computer access warrant

The increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms can adversely impact ASIO's ability to execute a computer access warrant for the purpose of obtaining access to data relevant to security.

Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.

To address this, section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.

Person searches

The ASIO Act currently contains the power to search a premises (section 25). Contained within this is the power to search a person who is *at or near* the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter (subsection 25(4A)).

Where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are *'at or near'* the premises specified in the warrant.

For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible. The existing limitation could be addressed by enabling ASIO to request a warrant to search a specified person rather than premises (subject to existing safeguards in subsections 25(4B) and 25AA) so that there would be sufficient operational flexibility while maintaining appropriate accountability via the warrant process.

Authorisation lists for warrants

Section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.

The requirement to maintain a list of the individual names of each officer who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons.

The problem could be overcome in large part if the Director-General could approve classes of people to execute a warrant. For example, the Director-General could authorise officers of a certain level within a particular Division of ASIO. Such persons at any one time would be readily ascertainable ensuring the level of accountability is not diminished, while improving operational efficiency.

3.3 Clarify ASIO's ability to cooperate with the private sector

Subsection 19(1) of the ASIO Act enables ASIO to cooperate with authorities of the Commonwealth, as well as Departments, police forces and authorities of the States, where it is necessary or conducive to the functions of ASIO. It is unclear whether section 19 could be read to imply that ASIO should not cooperate with organisations outside of government.

This concerns ASIO given the important role the private sector plays in Australia's national security, including by owning and operating a significant proportion of Australia's critical infrastructure. Furthermore, it is conducive to ASIO's functions to cooperate with the private sector. For example, ASIO's Business Liaison Unit (BLU), provides an interface between Australian business and the Australian Intelligence Community. The BLU provides intelligence backed reporting that can be used for risk management decision making. Such reports include reporting on the current security environment and threats to particular industry sectors.

It may be desirable to amend subsection 19(1) to avoid any doubt about ASIO's ability to cooperate with the private sector.

3.4 Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act

Section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. In particular, information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment exceeding 12 months). Section 92, which makes it an offence for a person to publish the identity of an ASIO officer, is punishable by 12 months imprisonment. By virtue of section 18, ASIO is precluded from passing information about the possible commission of this offence to law enforcement agencies.

4. Matters on which the Government expressly seeks the views of the PJCIS

4.1 Modernise and streamline ASIO's warrant provisions

Use of third party computers and communications in transit

The ASIO Act recognises the importance of ensuring ASIO is able to access computers where necessary for the performance of its statutory functions and where approved by the Attorney-General.

However, advancements in technology have made it increasingly difficult for ASIO to execute its computer access warrants. Where a target is security conscious, innovative methods of achieving access to the target computer have to be employed. In the same way that access to a third party premises may be necessary to execute a search warrant, it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant.

To overcome this problem, it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer. Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.

Incidental Entry

Sections 25 and 25A of the ASIO Act currently enable an officer, in the execution of a search or computer warrant, to do any thing that is reasonably incidental to the exercise of powers under that warrant. It is not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant. Additionally, it may be necessary to enter a third party premises for the purposes of installing a surveillance device. Clarification of the scope of the incidental power would assist ASIO in executing search and computer warrants.

Use of force

Subsections 25(7), 25A(5A), 26B(4) and 26C(4) relate to the use of force when exercising a power under a warrant and when entry into a premises is authorised under the warrant. The headings to each of those subsections suggest that the powers in those subsections are limited to entry to the target premises. The provisions relating to use of force are not limited in such a way. Technical amendments may therefore be necessary to correct this drafting anomaly.

Evidentiary Certificates

Currently, protecting information that reveals sensitivities about the identity of ASIO officers and capabilities used in the course of exercising special warrant powers relies on successful public interest immunity claims or, where available, orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004*. Unlike the *Telecommunications (Interception and Access Act) 1979* (TIA Act) and the *Surveillance Devices Act 2004* (SD Act), there is no consistent regime to protect ASIO information, capabilities and officer identities under the ASIO Act.

An evidentiary certificate regime could be introduced in the ASIO Act, similar to those which exist under the TIA and SD Acts, to provide a legislative basis for assisting ASIO to protect the identity of officers and sensitive capabilities involvied in the execution of warrant powers.

4.2 Amend the Intelligence Services Act 2001

Australia's foreign intelligence agencies, ASIS, DSD and DIGO, collect intelligence in accordance with requirements set by Government and operate under the IS Act. These agencies have identified problems arising out of the operation of the IS Act, which are considered below.

Ministerial Authorisations

The IS Act imposes strict controls on the ability of those agencies to produce intelligence on an Australian person. The Minister responsible for each Australian foreign intelligence agency is required to direct that the agency obtain authorisation from the Minister before undertaking an activity, or a series of activities, for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person.

Before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied under section 9(1) that:

- any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned, and
- there are satisfactory arrangements in place to ensure that
    - nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency, and
    - the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

According to section 9(1A)(a), before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied that the Australian person is, or is likely to be, involved in one or more of the following activities:

- activities that present a significant risk to a person's safety;
- acting for, or on behalf of, a foreign power;
- activities that are, or any likely to be, a threat to security (for this ground the Minister must also obtain the agreement of the Attorney-General);
- activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
- committing a serious crime by moving money, goods or people;
- committing a serious crime by using or transferring intellectual property;
- committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy; and
- activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law.

These activities do not specifically cover the situation where a person is or is likely to be involved in intelligence or counter-intelligence activities.

A new item could be added to the list in section 9(1A)(a) of the IS Act which would allow the Minister to give an authorisation if he or she is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities. This would allow the Minister to issue an authorisation where the current grounds, for example, 'activities that present a significant risk to a person's safety,' are not available because the risk is to ASIS operations or is not specific to a person's safety.

In particular, this would assist ASIS to perform its existing function of conducting counter-intelligence activities under section 6(1)(c) of the IS Act and allow DSD and DIGO, at the request of ASIS and with approval from their Minister, to assist ASIS. In turn this would enable these agencies to protect their operations and those involved in them by allowing the agencies to produce intelligence on a person who the Minister is satisfied is, or is likely to be, involved in intelligence or counter-intelligence activities. This activity may detect the interference of a foreign power, in which case ASIO would normally become involved in assessing any threat to security.

It is imperative that Australia's intelligence agencies are appropriately equipped to protect Australia's vital national security interests. This includes the ability for Australia's foreign intelligence and security services to interact and work seamlessly together.

In March 2011, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* made amendments to the ASIO Act and the IS Act to enable Australia's intelligence agencies to more closely cooperate and assist one another in the performance of each other's functions. Specifically, section 13A of the IS Act was introduced to facilitate greater cooperation in multi-agency teams, such as under the Counter Terrorism Control Centre, which is hosted by ASIO, and enable agencies to harness resources in support of key national security priorities.

However, there are differences in the legislative regimes which apply to ASIS, DSD and DIGO under the IS Act and to ASIO under the ASIO Act when they produce intelligence on Australian persons. In part these differences reflect the different nature and functions of the IS Act agencies and ASIO. When the agencies are cooperating and assisting ASIO in the performance of ASIO's functions, these differences have led to situations being identified where ASIO is able to undertake an activity for the purposes of its functions but an agency subject to the IS Act may not be able to fully cooperate with and assist it.

To better meet the intention of enabling Australia's intelligence agencies to cooperate and assist each other in the performance of each other's functions to protect Australia and Australians, section 13A of the IS Act could be amended. For example, section 13A could be amended to enable the Minister responsible for an IS Act agency to authorise specified activities where the agency is cooperating with ASIO in the performance of an ASIO function.. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required. This change would create greater consistency between the ministerial approval regime that applies to the IS Act agencies and the approval regime which applies to ASIO.

The proposal is principally intended for ASIS and ASIO cooperation relating to the capabilities, intentions and activities of people or organisations outside Australia. Given existing Defence agencies' functions and capabilities, and the nature of the activities to which the proposal is sought to address, it is unlikely that Defence would utilise the proposed change.

The existing safeguards in the IS Act could apply to the proposed section 13A authorisation. These include the requirement for all ministerial authorisations to be provided to the IGIS who oversees the legality and propriety of the operations of the intelligence agencies. Additionally, the communication and retention of intelligence collected under the ministerial authorisation would be subject to the Privacy Rules.

The proposed changes to section 13A could also operate in a limited set of circumstances:

- A ministerial authorisation under the proposed changes to section 13A would usually only be issued for a discrete activity for a specified purpose where ASIS is cooperating with ASIO in connection with the performance of its functions. This category of ministerial authorisation will not be able to be issued to ASIS, DSD and DIGO to assist another IS Act agency, or a prescribed Commonwealth authority, or a State authority.
- A ministerial authorisation under section 13A will not replace the need to obtain a warrant where a warrant would currently be required under the ASIO Act or the TIA Act.
- Renewal could be sought, but where a ministerial authorisation under a section 9(1A) ground could be sought, further ministerial authorisation would need to be sought under sections 8 and 9 of the IS Act rather than as a renewal of the section 13A authorisation.

ASIS co-operation on self-defence and weapons training

ASIS operates in a number of very dangerous locations overseas. In recognition of this, the IS Act was amended in 2004 to enable ASIS staff members and agents to receive training in the use of weapons and self-defence techniques, subject to a number of important safeguards (schedule 2).

However, under this regime, ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. The IS Act does not currently enable ASIS staff members to participate in joint training in the use of weapons with persons cooperating with ASIS, even though ASIS staff members are authorized to use weapons to protect such persons. At a practical level, the current inconsistency restricts joint training activities because ASIS trainers cannot run training that includes individuals who are not ASIS staff members.

Such cooperation would not enable ASIO officers to carry weapons or receive training from ASIS in the use of weapons. Co-operation on weapons training would be limited to Commonwealth, State and Territory bodies that have, under some other law, a right to carry weapons in the course of their duties. This will cover training with law enforcement and military personnel.

Such cooperation would enable ASIS to cooperate with a limited number of approved overseas authorities in the delivery of training in self defence and weapons. Such cooperation could be limited to authorities approved by the Foreign Minister under section

13(1A) of the IS Act. Such an approval requires the Foreign Minister to first consult with the Prime Minister and Attorney-General.

5. Next Steps

This Chapter has discussed the Australian Intelligence Community legislative reform aspect of the package of reform proposals referred to the PJCIS for inquiry and consultation. The Government recognises that some of the reforms are controversial and may attract significant media interest. To avoid public misunderstanding as to the nature of these reforms, it is imperative that the PJCIS take into account a wide range of views on the proposals from public stakeholders and government agencies. This will ensure that any measures brought forward to enhance the intelligence gathering capabilities of our intelligence agencies continue to be subject to appropriate checks and balances on these powers.

CONCLUSION

The preceding chapters of this Discussion Paper have elaborated on the complex international security environment in which our intelligence and law enforcement agencies operate. Ideas for telecommunications interception reform (Chapter 2), telecommunications sector security reform (Chapter 3) and Australian intelligence community reform (Chapter 4) seek to equip these agencies with the capability to meet today's emerging national security challenges.

In light of the issues discussed, the Government seeks the views of the PJCIS on the package of ideas. This Discussion Paper will prove useful as a basis for stakeholder consultation. A number of key industry representatives and Government agencies will seek to provide their views on the proposals to the PJCIS.