QTB13/28

DATA RETENTION

Issue: On 24 June 2013 the Parliamentary Joint Committee on Intelligence and Security handed down its report entitled Report of the Inquiry into Potential Reforms of Australia's National Security Legislation. The report noted that there was a "diversity of views" among Committee members on the establishment of a mandatory data retention regime, concluding that the decision was a matter for Government

Key points

- I note the findings of a report by the Parliamentary Joint Committee on Intelligence and Security in June 2013 which includes recommendations in relation to data retention.
- The Government will carefully consider the Committee's recommendations before making any decisions about data retention.

If asked about the Committee's recommendations

- The Committee ruled out any regime which included data about content or internet browsing data.
- The Committee ruled out retention periods longer than two years. Moreover, it offered specific guidance on the need for robust oversight, review and reporting arrangements.

If asked about the importance of data retention

- The Government will always seek to help our law enforcement agencies. Data retention can help to corroborate a person's identity and address and be used to establish relationships between criminals.
- During presentations to the Committee, our Police Commissions made it clear that data is critically important to their investigations.
- Phone companies already retain this information. However, with changes to billing practices they need to retain less data for shorter periods.

Clearance officer: Geoff McDonald Phone: 6141 2875
Division: NSLPD
Date Updated: 31/10/2013

Background

Former Attorney-General Roxon referred a variety of matters to the PJCIS on 30 April 2012. Data retention was included in that referral.

The data retention proposal has been the subject of ongoing public and media criticism. Data retention has been discussed publically since at least 2006 when the EU Data Retention Directive (2006/24/EC) was adopted by the European Union. Data retention became a controversial issue in Australia in June 2010 when meetings that the Attorney-General's Department held with certain telecommunications providers attracted public scrutiny.

On 24 June 2013 the Parliamentary Joint Committee on Intelligence and Security handed down its report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The Committee expressed a range of views and made 43 recommendations, including:

- Expressing broad support for reform of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and specific proposals such as creating a single warrant and allowing for attribute interception
- Noting that there was a "diversity of views" among Committee members on the establishment of a mandatory data retention regime, concluding that the decision was a matter for Government
- Recommending the Government proceed to amend the *Telecommunications Act 1997* to provide a telecommunications security framework, and
- Supporting the majority of the proposed measures to modernise and improve laws relating to Australian intelligence agencies.

The Department is yet to advise the Government on recommendations in the report.

Proposed Telecommunications Interception Reform

- The *Telecommunications (Interception and Access) Act 1979* is drafted on now obsolete assumptions about communications technology and industry structure. The Act's privacy protections and lawful access regime are inadequate for the modern telecommunications environment.
- The PJCIS inquiry recommended comprehensive review of the Act in consultation with interested stakeholders, with exposure draft legislation released for public consultation.
- The PJCIS endorsed:
  - Clear protection for the privacy of communications
  - The creation of a single warrant allowing for 'attribute' interception
  - Legal provisions which are technology neutral and clarify the industry assistance obligations
  - Robust oversight and accountability which supports administrative efficiency

TI Reform – Data Retention

- Telecommunications service providers are increasingly not retaining non-content information about telecommunications (telecommunications data), due to changes in technology and their business practices.
- Telecommunications data establishes the identity of suspects and their communications networks, particularly at early phases of investigations.
- The PJCIS recommended that if government is persuaded to pursue a mandatory data retention regime, draft legislation should be referred to the PJCIS for examination.

HOT TOPIC BRIEF **NSCJG-17**

NSCJG-17 – Response to the PJCIS Inquiry into national security reforms, including data retention

On 24 June 2013 the Parliamentary Joint Committee on Intelligence and Security handed down its report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The Committee expressed a range of views and made 43 recommendations, including:

- Expressing broad support for reform of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and specific proposals such as creating a single warrant and allowing for attribute interception
- Noting that there was a "diversity of views" among Committee members on the establishment of a mandatory data retention regime, concluding that the decision was a matter for Government
- Recommending the Government proceed to amend the *Telecommunications Act 1997* to provide a telecommunications security framework, and
- Supporting the majority of the proposed measures to modernise and improve laws relating to Australian intelligence agencies.

Government is yet to respond to the Report.

Key messages

- The Department welcomes the Report of the Parliamentary Joint Committee on Intelligence and Security.
- Government has not yet responded to the Committee's Report.
- The Committee considered hundreds of written submissions in addition to oral submissions, in public and in camera, before making its carefully considered recommendations.
- The Department acknowledges and supports the Committee's recognition of the need for Australia's security and intelligence agencies to be appropriately resourced and to be granted powers, which are often intrusive, to carry out their work.
- The Department agrees with the Committee that intrusive powers must always be balanced by appropriate safeguards for the privacy of individuals and the community.
- The Department is currently working on proposed responses for the Government's consideration on different elements of Report.

  The Department believes that the Committee's report forms a 'road map' specifying how each matter is best progressed.

6

- The Government notes the Committee's view that a holistic review of the legislation is necessary to ensure the tools and the protections set out in the TI Act reflect the way in which the contemporary communications environment operates.
- The Department notes that the Committee supported the majority of proposed measures to improve laws relating to Australian intelligence agencies.

  The Department is now providing briefing to Government on options for progressing the Committee's recommendations.
- The Department notes the Committee's recommendation that a security framework for the telecommunications sector be established to ensure it is robust and resilient and is in the process of receiving a wide range of briefings, consistent with an incoming government.

AUSTRALIAN INTELLIGENCE COMMUNITY LEGISLATIVE REFORM

[If asked: what did the Committee recommend?]

- The Committee considered a range of measures to improve legislation governing the Australian Intelligence Community, which will allow those agencies to adequately deal with the challenges presented by the current and evolving security environment.
- Key recommendations include:
  - Creating an authorised intelligence operations scheme for the Australian Security Intelligence Organisation, subject to appropriate safeguards and accountability arrangements
  - Various amendments to improve the administration and efficiency of the warrant provisions in the ASIO Act, including, for example, a more efficient renewal and variation process, establishing a multiple powers warrant, establishing a class of persons to be able to execute a warrant, and clarifying various powers in warrant provisions relating to entry to third party premises
  - Introducing an evidentiary certificate regime to protect the identity of officers, sources and sensitive operational capabilities from disclosure in open court
  - Introducing new ministerial authorisation grounds in the *Intelligence Services Act 2001*

7

- Allowing the Australian Secret Intelligence Service (ASIS) to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

- The Government is currently receiving briefing on the detail of recommendations made by the Committee.
- It would be inappropriate to speculate on any steps we may take in the absence of a formal Government response.

[If asked: will there be any reforms to legislation governing the Australian Intelligence Community?]

- The Government is currently receiving briefing on the detail of the recommendations made by the Committee.
  - It would be inappropriate to speculate on any steps we may take in the absence of a formal Government response.
- I note, however, that a number of the recommendations made by the Committee involve legislative reform.

TELECOMMUNICATIONS INTERCEPTION REFORM

- The Committee was asked to consider proposals seeking to modernise and simplify the 34 year old interception regime and to better assure the privacy of Australians and protect the social and economic wellbeing of the nation.
- The Department agrees with the Committee that a holistic review of the legislation is necessary to ensure the tools and the protections set out in the TI Act reflect the way in which the contemporary communications environment operates.
- The TI reforms seek to ensure the telecommunications interception regime continues to allow intelligence and law enforcement agencies to operate in a modern-day telecommunications environment.
- The TI reform proposals are not about expanding the powers of these intercepting agencies, these reforms are designed to ensure agencies can continue to do tomorrow what they can currently do today.
- No government decisions have been made about progressing the TI reform proposal.

8

Data retention

- No Government decision has been made about data retention.
- The Department acknowledges that there was a diversity of views within the Committee about the mandatory data retention proposal.
- The Committee recommended that, subject to a government decision, an exposure draft of proposed legislation be referred to the Committee for examination.
- The Committee also provided guidance on particulars of any regime, including that internet browsing data should be excluded, the retention period should not be more than 2 years, and that robust oversight, review and reporting arrangements should be put in place.
- Agencies stressed in their evidence to the Committee the importance of data availability to law enforcement and national security capability.

  Data forms an essential part of very many law enforcement and national security investigations.
- The Department will carefully consider the guidance of the committee before making any decisions in relation to data retention.

[If pressed, about the particulars of the need for data retention or the details of data retention]

I reiterate that the Government has not made a decision data retention regime and that the Committee's specific guidance on both consultation and the particulars of any regime will be carefully considered.

No data retention regime would involve the content of emails, texts or social media messaging.

Rather, it relates to who contacted whom and when.

Data can be used to corroborate a person's identity and address, and can be used to establish relationships between criminals.

Phone companies retain this information now, but need less data for shorter periods because billing practices are changing.

During their presentation to the Committee, the AFP, NSW and SA Police Commissioners made it very clear that data is fundamentally important to their investigations and that

9

some leads are now failing because carriers are deleting that data more regularly than they have done in the past.

Other countries have taken the approach of requiring phone companies to keep certain kinds of data.

The Government will consider the Committee's specific recommendations about data retention before making any decisions.

TELECOMMUNICATIONS SECTOR SECURITY REFORM

[If asked: What did the Committee recommend?

- The Committee understood the rationale for the telecommunications sector security reform proposal and recommended (rec 19) the establishment of a security framework for the telecommunications sector noting warm, if cautious, support from industry.
- The security framework recommended includes:
  - a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised access and interference
  - a requirement for members of industry, where requested to provide Government with information to assist in the assessment of national security risks to telecommunications infrastructure
  - powers of direction and a penalty regime to encourage compliance with the security framework
- The Committee further recommended, through the development of a Regulation Impact Statement (RIS), the Government consider issues impacting on industry, including:
  - the interaction of the proposed regime with existing legal obligations on corporations;
  - consideration of good faith provisions in the framework; and
  - impacts on competition in the marketplace, including potential barriers to entry for lower cost providers.
- The Department is preparing a Regulation Impact Statement taking into account these considerations.

[If asked: what does TSSR entail?]

- The telecommunication sector security reforms aim to introduce a security framework to manage national security risks to Australia's telecommunications sector, by encouraging industry to build national security considerations into its business and investment decision making.
- Under the current regulatory environment there is no enforceable obligation on the telecommunications industry to protect its networks and infrastructure, nor does industry have access to sensitive national security information to adequately assess emerging threats and risks to its infrastructure.

10

- Under the proposed security framework, industry would have the flexibility to decide what measures it needs to take to meet its obligations, as well as complying with Government's national security expectations.
- The only current statutory means for the management of national security risks presented through telecommunications services is for the Attorney General to issue a direction to a carrier or carriage service provider to cease a service.
- The security framework would include more proportionate means for government intervention including powers of direction, enforceable by financial penalties, where security outcomes are unable to be achieved.

Does the Government agree with the recommendation to establish a security framework for the telecommunications sector and when will it respond?

- As the Committee notes, it is important that implications such as competition impact and regulatory overlap are considered as part of a Regulation Impact Statement.
- Work is well underway on a Regulation Impact Statement that will inform Government's consideration about the security framework.
- As can be expected of an incoming government, it is in the process of receiving a considerable number of briefings including on national security matters.

Version #: 2	Cleared by: Geoff McDonald	Action officer: S22(1)
Current at: 14 November 2013	Phone number: 6141 2875	Action officer number: S22(1)

Return to Index

Response

Telecommunications Sector Security Reform (TSSR)

The problem

- S33(a)(i)
- The telecommunications sector is changing – suppliers are now offering to operate layers of the network rather than just selling equipment
- S22(1)
-

Response

TSSR (continued) *Current situation*

- At present, the only legislative provision is for the Attorney-General to direct a carrier or provider to cease a service on security grounds. Regulation needs to be "lighter touch".
  - Currently, security agencies rely on informal collaboration to promote the management of security risks
- The draft security framework (endorsed by the PJCIS) would promote a closer relationship between government and carriers / providers, while still providing opportunities for all suppliers
- AGD has developed a draft security framework (yet to be considered by Government) which comprises:
  - a universal obligation for industry to protect its networks and facilities from unauthorised access or interference; and
  - graduated steps for intervention through directions, enforced with penalties

SECRET, SENSITIVE
AUSTEO

Australian Government
Attorney-General's Department

Sub No: AG-SB2013/1799
File No: 12/1024
ATTORNEY-GENERAL

Date submitted to Office by AGD: _____
Min No:

Subject: Telecommunications Sector Security Reform

Deadline: None, this submission may be considered with AG-SB2013/1737.

Key Issues: To date, Government's management of national security risks to the telecommunications sector S33(a)(i)

The only statutory recourse for addressing security concerns is a direction under section 581(3) of the *Telecommunications Act 1997* to cease a service [Attachment A]. S33(a)(i)
S33(a)(i)

S22(1)

highlight the absence of a proportionate statutory basis for government intervention based on security concerns. The Minister for Communications has publicly expressed his interest in revisiting the decision on Huawei's access to NBN work. S47C(1)
S47C(1)

AGD Analysis: Changes in technology and the market continue to occur at a rapid pace in Australia. It is envisaged that this environment will give rise to continuing security risks S33(a)(i)
S33(a)(i)

S33(a)(i)

S33(a)(i) In the current telecommunications regulatory environment there is a lack of visibility and awareness about the harm caused to victims (customers) of cybercrime and security lapses. For example, a customer is often unaware that a data spill with their information has occurred and even less so the consequences of their personal and financial information being accessed. S33(a)(i)
S33(a)(i)

S33(a)(i)

A security framework (Telecommunications Sector Security Reform) has been developed by AGD (and was recommended by PJCIS) as a means to enable more consistent, transparent and sustainable management of security issues between government and industry. S33(a)(i)
S33(a)(i)

S33(a)(i) A security framework would be achievable by amending the Telecommunications Act. As the Minister for Communications is responsible for this Act and significant procurement decisions for the supply

of equipment and services to the NBN, AGD has been working closely with his Department about possible legislative changes. AGD has been developing draft guidelines for industry on the reform package which outline Government's expectations under a security framework and the Department is seeking to test these with industry. The draft guidelines establish principles drawing on recognised international information security good practice.

S33(a)(iii)

S33(a)(i) New Zealand has introduced legislation to establish a security framework S33(a)
S33(a)(i)

Recommendation: I recommend that you:

a) S47C(1) **Agreed / not agreed / discuss**

b) **Agreed / not agreed / discuss**

c) **Agreed / not agreed / discuss**

.....
Andrew Rice
AS, Cyber and Identity Security Policy Branch
6141 2704
/ /2013

.....
Attorney-General
/ /2013

Cleared by:

Mike Rothery	Tony Sheehan	Roger Wilkins AO
FAS, NSRPD	Deputy Secretary	Secretary
/ /2013	/ /2013	/ /2013

Action Officer: S22(1) 21/10/2013

SECRET: SENSITIVE
AUSTEO

Background

S33(a)(i)

S33(a)(i) telecommunications carriers and carriage service providers will continue to be driven by changes to the market through the National Broadband Network roll-out (NBN) and further technological innovation.

S22(1)

Telecommunications Sector Security Reform

4. S33(a)(i)
S33(a)(i) The Attorney-General's Department (AGD) has subsequently developed a risk based regulatory framework (security framework) as an effective and sustainable way to mitigate national security risks. The Telecommunications Sector Security Reforms (TSSR) were included in a suite of proposed reforms before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in 2012. The proposed framework targets Carriers, Carriage Service Providers and Carriage Service Intermediaries (C/CSPs). They are best placed to influence security considerations, either directly or through service obligations of commercial contracts with their suppliers of equipment and services given their visibility of networks and position in the supply chain S33(a)(i)
S33(a)(i)

5. The framework proposes amendments to the *Telecommunications Act 1997* to establish:

a) an obligation on C/CSPs to protect their networks and facilities from unauthorised access or interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;

b) 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

c) a graduated determination and penalty scheme to ensure compliance.

6. The proposed security framework would supplement and provide a proportionate means for government intervention where there are security risks presented by unauthorised access or interference to networks and facilities. The existing provision under section 581(3) of the Telecommunications Act (**Attachment A**) was introduced in 2004 and would remain available for risks to security presented by telecommunications services. Under this provision the Attorney-General, in consultation with the Prime Minister and Minister for Communications, may direct a C/CSP to not use or supply, or cease using or supplying, particular services where such use or supply would be prejudicial to security. As the direction only applies to a service as a whole it cannot be used to restrict service use or supply to a particular organisation, group or person. S33(a)(i)
S33(a)(i)

7. The proposed security framework seeks to place a universal obligation on all C/CSPs to maintain and demonstrate supervision and effective control of networks and facilities, and information in their control. While the obligation itself provides for an even-playing field, Government will engage more intensively with some C/CSPs based on assessment of threat and risk, taking into account market share, customers, and other elements of criticality to the national interest.

S22(1)

9. TSSR is not designed to exclude suppliers from accessing the Australian telecommunications market. While opportunities would continue to exist for all suppliers operating within the context of the security framework, S33(a)(i) S33(a)(i) to enable them to meet their regulatory obligations, to ensure the security and integrity of Australia's telecommunications infrastructure.

Draft Guidelines for Industry

10. AGD is developing guidelines (administrative) should Government agree to proceed with a new regime to assist industry understand and comply with the proposed new regulatory requirements. It is envisaged there will be several sets of Guidelines for Industry and 'fact sheets' but this needs to be tested with industry further. S33(a)(i) S33(a)(i) . Fact sheets would be developed for sub-sets of the telecommunications sector, such as back-haul (infrastructure) providers and resellers that identify how the universal obligation and management of security risks applies.

International Approaches

S33(a)(i)

S33(a)(i) At one end of the spectrum, the UK agreed to the development of a 'secure cell' to review Huawei equipment after agreeing to Huawei supplying equipment for British Telecom's 21st Century Network. The House of Commons' Intelligence and Security Committee in its report into foreign involvement in the UK's Critical National Infrastructure in June 2013 was critical of the way that national security issues were managed by officials, in isolation from Ministers. S33(a)(i)

S33(a)(i) Closer to Australia is the approach being progressed in New Zealand whose Parliament is considering legislation that would give effect to a security framework to manage security outcomes in a similar way to the proposed TSSR and S33(a)(iii) S33(a)(iii)

S47C(1)

Consultation

13. ASIO, Australian Signals Directorate, Department of the Prime Minister and Cabinet, and Department of Communications.

Sensitivities and Communication Plan

14. None. Any discussions will be commercial-in-confidence.

Attachment

- Attachment A: Section 581, *Telecommunications Act 1997*

TELECOMMUNICATIONS ACT 1997 - SECT 581

Power to give directions to carriers and service providers

(1) The ACMA may give written directions to:

(a) a carrier; or

(b) a service provider;

in connection with performing any of the ACMA's telecommunications functions or exercising any of the ACMA's telecommunications powers.

(2) This section is not limited by any other provision of a law that:

(a) confers a function or power on the ACMA; or

(b) prescribes the mode in which the ACMA is to perform a function or exercise a power; or

(c) prescribes conditions or restrictions which must be observed in relation to the performance by the ACMA of a function or the exercise by the ACMA of a power.

(3) If:

(a) a person who is a carrier or carriage service provider proposes to use, or uses, for the person's own requirements or benefit, or proposes to supply, or supplies, to another person, one or more carriage services; and

(b) the Attorney-General, after consulting the Prime Minister and the Minister administering this Act, considers that the proposed use or supply would be, or the use or supply is, as the case may be, prejudicial to security;

the Attorney-General may give to the carrier or carriage service provider a written direction not to use or supply, or to cease using or supplying, as the case may be, the carriage service, or all of the carriage services.

(3A) A direction under subsection (3) must relate to a carriage service generally and cannot be expressed to apply to the supply of a carriage service to a particular person, particular persons or a particular class of persons.

(4) A person must comply with a direction given to the person under subsection (1) or (3).

(5) In this section:

"security" has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

S22(1)

S22(1) A security framework has been developed for the telecommunications sector, something the Parliamentary Joint Committee on Intelligence and Security recommended be established in June 2013. A separate submission provides further detail on this approach [AG-SB2013/1799].

S33(a)(iii)

S33(a)(iii) New Zealand has introduced legislation to establish a security framework S33(a)(iii) S22(1)

S22(1)

S22(1) As changes in technology and the market continue to occur at a rapid pace in Australia,

S33(a)(i)

SECRET, SENSITIVE
AUSTEO

Recommendation: I recommend that you:

a) S22(1) **Noted / discuss**

b) **Noted / discuss**

Andrew Rice
AS, Cyber and Identity Security Policy Branch
6141 2704
22 / 10 /2013

Attorney-General
10 / 11 /2013

Cleared by:	Mike Rothery FAS, NSRPD 22/10 /2013	Tony Sheehan Deputy Secretary / /2013	Roger Wilkins AO Secretary / /2013
Action Officer: S22(1)	21/10/2013		

SECRET, SENSITIVE
AUSTEO

Background

S33(a)(i)

S33(a)(i) telecommunications carriers and carriage service providers will continue to be driven by changes to the market through the National Broadband Network roll-out (NBN) and further technological innovation.

S22(1)

Telecommunications Sector Security Reform

S22(1)

S22(1) The Attorney-General's Department (the Department) has subsequently developed a risk based regulatory framework (security framework) as an effective and sustainable way to mitigate national security risks. The Telecommunications Sector Security Reforms (TSSR) were included in a suite of proposed reforms before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in 2012. The proposed framework targets Carriers, Carriage Service Providers and Carriage Service Intermediaries (C/CSPs). They are best placed to influence security considerations, either directly or through service obligations of commercial contracts with their suppliers of equipment and services given their visibility of networks and position in the supply chain.S33(a)(i)

S33(a)(i)

5. A further submission sets out further information about the Telecommunications Sector Security Reforms.

S22(1)

7. TSSR is not designed to exclude suppliers from accessing the Australian telecommunications market. Opportunities would continue to exist for all suppliers operating within the context of the security framework. All suppliers would continue to compete in the broader market and price competition should remain.S33(a)(i)

S33(a)(i) to enable them to meet their regulatory obligations, to ensure the security and integrity of Australia's telecommunications infrastructure.

International Approaches

S33(a)(i)

S33(a)(i) At one end of the spectrum, the UK agreed to the development of a 'secure cell' to review Huawei equipment after agreeing to Huawei supplying equipment for British Telecom's 21st Century Network. The House of Commons' Intelligence and Security Committee in its report into foreign involvement in the UK's Critical National Infrastructure in June 2013

~~AUSTEO SECRET SENSITIVE~~

~~AUSTEO~~

was critical of the way that national security issues were managed by officials, in isolation from Ministers.
S33(a)(i)

S33(a)(i)
S33(a)(iii)
S33(a)(iii) At the other end of the spectrum, the New Zealand Parliament is currently considering a bill that would give effect to a security framework that would manage security outcomes in a similar way to the security framework recommended by the PJCIS.
S47C(1)

Consultation

10. ASIO, Australian Signals Directorate, Department of the Prime Minister and Cabinet, and Department of Communications.

Sensitivities and Communication Plan

11. None. Any discussions will be commercial-in-confidence.

~~SECRET SENSITIVE~~

~~AUSTEO~~

Document 10

QTB 13/30

TELCOMMUNICATIONS SECURITY

Issue: Measures the Australian Government is taking to manage national security concerns in the telecommunications sector. Rapid developments in both technology and the market, driven by the roll out of the National Broadband Network, are placing heightened pressure on telecommunications carriers and carriage service providers to make business decisions about the supply of equipment and managed services that may present national security risks to both infrastructure and the data held and carried across it.

S22(1)

Key points

- The threat of espionage and sabotage through cyber-attacks targeting both government and industry is real.
- These types of attacks through Australia's telecommunications networks and facilities have the potential to cause considerable damage to our national interest.
- They also undermine the confidence and integrity of Australian's use of telecommunications networks and data.
- Australian security agencies currently rely on cooperation from telecommunications carriers and carriage service providers to manage security risks presented by suppliers of equipment and services.
- In this, as with all activities of Australia's security agencies, all cooperation is conducted in strict accordance with relevant laws.

What is the government going to do about security to telecommunications?

- The Government is continuing to take briefings from security agencies on the security of telecommunications networks.
- The Government notes the recommendation from the Parliamentary Joint Committee on Intelligence and Security that a security framework be established to more effectively safeguard infrastructure and data.
- The Government further notes the Committee found warm, if cautious, support from the telecommunications industry for a security framework.
- The Government notes the Committee's view that a framework would encourage those operating within the industry to more actively engage

Clearance officer: Andrew Rice Phone: 6141 2704
Division: NSRPD
Date Updated: 31/10/2013

with Government and build national security considerations into their business and investment decision making.

Clearance officer: Andrew Rice Phone: 6141 2704
Division: NSRPD
Date Updated: 31/10/2013

QTB 13/30

Background

Telecommunications Sector Security Reform (TSSR)

The need to protect Australia's telecommunications infrastructure from unauthorised access, interference and sabotage has reached a critical point and it is becoming increasingly impetrative that a security framework be implemented to mitigate concerns.

In the current environment, there is no enforceable obligation on the telecommunications industry to protect its networks and infrastructure.

In June 2013, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended (rec 19) that the Government establish a security framework as part of proposed Telecommunications Sector Security Reforms (TSSR). The framework has received 'warm if' cautious' support.

The PJCIS recommendation for a security framework includes:

- a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised access and interference
- a requirement for members of industry, where requested to provide Government with information to assist in the assessment of national security risks to telecommunications infrastructure
- powers of direction and a penalty regime to encourage compliance with the security framework

The Committee further recommended, through the development of a Regulation Impact Statement (RIS), the Government consider issues impacting on industry, including:

- the interaction of the proposed regime with existing legal obligations on corporations;
- consideration of good faith provisions in the framework; and
- impacts on competition in the marketplace, including potential barriers to entry for lower cost providers.

The Department is preparing a Regulation Impact Statement taking into account these considerations.

International Developments

Many of our international partners and like-minded countries are taking similar approaches in managing risk to their critical telecommunications infrastructure.

In October 2013 the New Zealand Government passed its Telecommunications (Interception and Security) Bill, which contains a security framework that is very similar to the PJCIS recommendation for the TSSR.

Clearance officer: Andrew Rice Phone: 6141 2704
Division: NSRPD
Date Updated: 31/10/2013

Background

S22(1)

Telecommunication Sector Security Reforms (TSSR)

The Attorney-General's Department in consultation with ASIO and other agencies has been developing a security framework – the Telecommunication Sector Security Reforms (TSSR) – to address national security to concerns to Australia's telecommunications infrastructure. The security framework will enhance information sharing between Government and industry to mitigate risks and provide industry with the certainty and the flexibility it requires to make its business and investment decisions, whilst remaining compliant with the security framework. On 24 June 2013, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled its report into potential reforms of National Security Legislation which included the TSSR. The Report supported the TSSR and recommended (rec 19) the development of a security framework to mitigate national security risks to Australia's telecommunications infrastructure.

For further information see **QTB 13/25** – Telecommunications Security.

Clearance officer: Andrew Rice Phone: 6141 2704
Division: NSRPD
Date Updated: 7/11/2013

***Page 1 of this document is exempt in full under section 47C(1) of the FOI Act (deliberative processes)

PROTECTED SENSITIVE: CABINET

COVERING SECRET CODEWORD

Background

2. On 24 June 2013, the PJCIS tabled its report into potential reforms of national security legislation, including reforms related to the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, the ASIO Act and the IS Act. The Committee began its inquiry on 9 July 2012 and received 240 submissions from interested members of the public and organisations as well as relevant Government Departments and agencies. The Committee also held a number of public and in camera hearings on the proposals between September and November 2012.

3. In relation to the proposed reforms to the ASIO and IS Acts, the PJCIS supported all but two proposals put forward to improve the efficiency and capabilities of agencies within the Australian Intelligence Community. In relation to proposals not supported by the PJCIS, one concerned increasing the maximum duration of search warrants and the other was to give ASIO the power to search a person independently of a premises search. s47C(1)