Australian Government

Department of Home Affairs

Telecommunications Sector Security Reforms

2018–19 Annual Report

Introduction

This is a report under subsection 315J(1) of the *Telecommunications Act 1997* (the Act) for the financial year ending 30 June 2019 on the operation of Part 14 of the Act, to the extent that Part was amended by the *Telecommunications and Other Legislation Amendment Act 2017* (commonly referred to as the Telecommunications Sector Security Reforms (TSSR)).

The TSSR amendments to Part 14 of the Act commenced on 18 September 2018. See *Background* below for further information on TSSR.

Information required under subsection 315J(1A) of the Act

Directions Powers

The Home Affairs Minister gave no directions under subsection 315A(1) in the financial year ending 30 June 2019.

The Home Affairs Minister gave no directions under subsection 315B(2) in the financial year ending 30 June 2019.

Notification obligation

The Communications Access Co-ordinator (CAC) received 34 notifications under subsection 314A(3) in the financial year ending 30 June 2019.[1]

In instances where the CAC did not require further information about a notified change, the average number of days taken to give a notice under subsection 314B(3) or (5) was 22 calendar days.

In instances where the CAC required further information about a notified change, the average number of days taken to give a notice under subsection 314B(1) requesting further information was 22 days. The average number of days taken to give a notice under subsection 314B(3) or (5) once further information was provided to the CAC was 27 calendar days.

The average number of days taken by the CAC after a notification was submitted under subsection 314A(3) to give a notice under subsection 314B(3) or (5), including days taken to request, receive and consider further information where applicable, was 52 calendar days.

One hundred percent of notices under subsection 314B(3) or (5) were given within the period under subsection 314B(6); that is, either within 30 calendar days of receiving the notification under subsection 314A(3) or if the CAC requested further information from the carrier or provider, as soon as practicable and within 30 calendar days of receiving that further information.

Further detail

Table 1 – Breakdown of notices given by the CAC under subsections 314B(3) and (5)

Type of notice	Number of notices issued
Subsection 314B(3) 'some risk'	28
Subsection 314B(5) 'no risk'	1

Note: *As at 1 July 2019, the were five notifications that the CAC had yet to respond to by giving a notice under subsection 314B(3) or (5); all such notifications were within the statutory timeframe to issue a response.*

[1] This figure does not include one notification that was subsequently withdrawn by the notifying carrier.

The CAC required further information about 16 notified changes, which was 47 percent of all notifications received during the reporting period.

Applications for exemption from the notification obligation

The CAC received one application under subsection 314A(5A) in the financial year ending 30 June 2019.

The CAC took 54 calendar days to give one notice under subsection 314A(4) or (5) or paragraph 314A(5B)(b) in response to the application that was received.

One hundred percent of such notices were given within the period under subsection 314A(5B); that is, within 60 calendar days of receiving the application.

Security Capability Plans

The CAC did not receive any security capability plans in the financial year ending 30 June 2019.

Information-gathering powers

The Home Affairs Secretary gave no notices under subsection 315C(2) in the financial year ending 30 June 2019.

Information sharing arrangements

The TSSR framework is intended to formalise and strengthen pre-existing informal engagement and information sharing practices between the telecommunications industry and Government. The aim is to encourage early engagement on proposed changes to systems and services that could give rise to a national security risk and collaboration on the management of those risks.

In the 2018–2019 financial year the Department participated in approximately 53 engagements to ensure industry understood their security and notification obligations and to provide advice on proposed changes to telecommunications systems or services.

While these discussions provide broad guidance to industry, notifications remain the most effective mechanism to share security information with industry. The Department works closely with security agency partners to assess notifications and to share threat advice with carriers to improve the overall security posture of the telecommunications industry.

The Department has developed a secure communication pathway to communicate sensitive information such as security threat advice to industry.

The Department also works closely with carriers to help them implement risk controls recommended in notices under subsection 314B(3). For example, the Department has participated in eight workshops to continue providing advice on the implementation of recommended mitigations.

Guidance Material

The Department has a dedicated TSSR webpage to facilitate information sharing with industry which contains TSSR guidance material including:

- administrative guidelines on TSSR
- fact sheets explaining the security and notification obligations
- FAQs
- examples of the types of changes that may trigger notifications
- sample notification and notification exemption forms.

The Department continues to broaden awareness of the TSSR obligations through outreach across the telecommunications industry.

Summary of any feedback or complaints

Engagement and feedback from industry has been generally positive as industry recognises the benefits of being able to access security related information from government and implement mitigations to protect critical business operations.

The Department has worked with certain carriers to explain the intent of the legislation, including that submitting notifications demonstrates that a carrier is doing its best to comply with its security obligation and ensures it is appropriately informed. As "even the most informed [carrier] is unlikely to have access to the most up to date threat information available to [the Department],"[2] submitting notifications ensures carriers can benefit from that information and can make appropriately informed decisions, no matter their size or sophistication.

The Department has published guidance material addressing when changes will meet the threshold for notification and has provided advice to carriers about whether a notification was required in specific instances.

Trends or issues

Noting TSSR has only been in operation since 18 September 2018, the below trends and issues have been identified.

5G networks

Following extensive review, guidance on 5G security was provided to Australian Carriers on 23 August 2018. The security guidance provided to Australian carriers relates to obligations under TSSR to protect Australian communications, including 5G networks, from unauthorised access and interference. The Department of Home Affairs continues to work closely with telecommunications operators to ensure they understand their TSSR obligations with respect to deploying and operating 5G networks and services.

Approach to the notification obligation

Carriers are engaging positively with the Department about their TSSR notification obligations, including by:

- engaging in discussions to understand when the notification obligation applies;
- providing detailed information about changes to telecommunications systems and services via notifications; and
- participating in workshops to ensure best practice implementation of mitigations recommended in notices.

Carriers that do not notify the CAC about their proposed changes risk missing out on relevant threat information and targeted security advice. Further, should a carrier not provide a notification where the Department has advised the threshold has been met, that carrier may risk non-compliance with its security obligation.

Insufficient level of detail in notifications

Carriers are working to understand the level of detail required in their notifications, particularly about access and control arrangements for third party vendors and service providers. Insufficient detail in notifications is the primary obstacle to shorter response times by the CAC.

The Department has updated the TSS1 notification form to ensure it collects relevant and targeted information from carriers and nominated carriage service providers about the proposed change. Where the CAC has issued a request for further information, the Department generally seeks to discuss with the carrier the intent of the request and the type of information being sought to undertake a comprehensive assessment.

[2] Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment Bill 2017 (Cth) [138].

In some instances, entities have notified the CAC very early in their planning for a change proposal. While early notifications are appreciated, in some circumstances the CAC may need to issue a notice that the proposed change carries risk, provide advice to the extent possible, and advise the entity to submit a further notification once the project is more advanced.

The Department is in the process of updating the guidance materials to better explain the level of detail required to conduct a comprehensive assessment and at what stage of a change proposal a notification should be submitted.

Background

The *Telecommunications and Other Legislation Amendment Act 2017*, known as the Telecommunications Sector Security Reforms (TSSR), amended the *Telecommunications Act 1997* (the Act) to establish a regulatory framework to better manage national security risks of espionage and foreign interference to Australia's telecommunications infrastructure.

TSSR commenced on 18 September 2018 following a 12-month implementation period.

Directions Powers

Section 315A and 315B of the Act allows the Minister for Home Affairs (the Minister), subject to safeguards, to direct a carrier or carriage service provider to:

- cease using or supplying carriage services where use or supply is considered to be prejudicial to security (section 315A).
- do, or not do, a specified act or thing where there is a risk of unauthorised interference with or unauthorised access to, networks or facilities that would be prejudicial to security (section 315B).[3]

The Minister can only exercise the direction powers where the Australian Security Intelligence Organisation (ASIO) has provided an adverse security assessment. An adverse security assessment is subject to the accountability requirements contained in Part IV of the *Australian Security Intelligence Organisation Act 1979*, including the provision of notice of the adverse security assessment to the subject of the assessment, and the availability of review in the AAT.

As a last resort power section 315A is intended to be used in the most extreme circumstances where the continued operation of the service would give rise to such serious consequences that the entire service needs to cease operating. The Minister must consult the Prime Minister and the Minister for Communications prior to giving written direction to cease operation of the service.

An additional safeguard under section 315B of the Act is that the Minister may only issue a direction if satisfied that all reasonable steps have been taken to negotiate, in good faith, with the carrier or carriage service provider to achieve an outcome of eliminating or reducing the security risk.

Notifications

Section 314A of the Act requires carriers and nominated carriage service providers to notify the CAC under subsection 314A(3) of their intention to implement a proposed change to a telecommunications service or telecommunications system if they become aware that implementing that change is likely to have a material adverse effect on the capacity of the carrier or provider to comply with its security obligations under section 313(1A).[4]

Once a notification has been received, a security assessment is completed in consultation with security agency partners. Within 30 calendar days of receipt of a notification, the CAC must provide the carrier with one of the following notices:

- **Further information** request under subsection 314B(1) detailing the required information for the CAC to assess whether there is a risk of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.

[3] 'Security' has the same meaning as in the *Australian Security Intelligence Organisation Act 1979* and among other things, covers the protection of, and of the people of, the Commonwealth and the States and Territories from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference.
[4] A change is likely to have a 'material adverse effect' if the proposed change may have an actual or measurable negative impact on the ability of the carrier or provider to comply with the duties in subsections 313(1A) or 313(2A) to protect networks from risks of unauthorised access and unauthorised interference.

- **Some risk associated** notice under subsection 314B(3) advising the carrier of a risk associated with the proposed change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security and recommending controls to mitigate the identified risk.
- **No risk** notice under subsection 314B(5) advising that the CAC is satisfied there is not a risk from the proposed change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.

Applications for exemption from the notification obligation

Carriers and nominated carriage service providers may seek a full or partial exemption from their obligation to notify the CAC of proposed changes to a telecommunications system or service. The CAC may grant an exemption under subsections 314A(4) or (5) of the Act. If a carrier submits a written application, the CAC must respond within 60 calendar days by either granting the exemption or refusing the exemption and providing written reasons for the refusal.

A carrier may apply to the Administrative Appeals Tribunal (AAT) for review of a decision by the CAC not to grant an exemption.

Security capability plans

Carriers and nominated carriage service providers may submit a security capability plan (SCP) each year to notify one or more proposed changes that are likely to have a material adverse effect on their capacity to meet their security obligation, as an alternative to notifying the CAC of each change individually.