Australian Government

Department of Home Affairs

Telecommunications Sector Security Reforms

2020–21 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 2021 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 2021.

The Home Affairs Minister gave no directions under subsection 315B(2) in the financial year ending 30 June 2021.

Notification requirement

The Communications Access Co-ordinator (CAC) received 30 notifications under subsection 314A(3) in the financial year ending 30 June 2021.[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 30 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 21 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 25 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 87 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.

[1] This figure does not include one notification that was subsequently withdrawn by the notifying carrier.

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'	24
Subsection 314B(5) 'no risk'	6

Note: *As at 1 July 2021, there were three notifications that the CAC had yet to respond to by giving a notice under subsection 314B (1) or 314B(3) or (5); all the three notifications were issued with a notice in July 2021 and within the statutory timeframe to issue the response.*

The CAC required further information about 22 notified changes, which was 73 percent of all notifications received during the reporting period.

Applications for exemption from the notification requirement

The CAC did not receive any applications under subsection 314A(5A) in the financial year ending 30 June 2021.

Security Capability Plans

The CAC did not receive any security capability plans in the financial year ending 30 June 2021.

Information-gathering powers

The Home Affairs Secretary gave no notices under subsection 315C(2) in the financial year ending 30 June 2021.

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 2020–2021 financial year the Department participated in 98 engagements to ensure industry understood their security and notification obligations and to provide advice on proposed changes to telecommunications systems or services. This activity included engaging with carriers who are yet to submit a notification, since TSSR came into effect.

The Department continues to use a secure communication portal to communicate sensitive information to industry, such as the risks and security advice associated with particular changes. A number of carriers have setup accounts on the portal, and other carriers will continue to be encouraged to do so.

Technical workshops and assistance

The Department continues to provide significant, in-depth technical guidance and assistance to carriers outside the formal notification process.

During the reporting period the Department held technical workshops with specific carriers to explore particular changes, discuss potential risks and provide guidance on designing and implementing targeted mitigations. This included ten workshops for the specific purpose of providing assistance with the implementation of mitigations suggested in notices under subsection 314B(3) or where further information is requested under subsection 314B(1).

The Department also considered a number of proposed changes during the reporting period outside the formal notification regime. While carriers determined that these changes did not meet the threshold for formal notification and chose to provide informal briefings to the Department, these briefings resulted often required an equivalent or even greater depth of technical analysis by the Department and security agencies than changes notified under section 314A. The Department is encouraged by an increase in the number of these engagements during the reporting period, as they foster stronger relationships with industry and support the Department's focus on working with industry to achieve positive security outcomes. The Department's regulatory objective is to achieve national security outcomes on a cooperative basis rather than through the formal exercise of regulatory powers.

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 periodically updates these materials, and works closely with industry to ensure that the materials are responsive to industry trends and requirements. The Telecommunications Sector Security Reforms (TSSR) Administrative Guidelines materials were last updated on 28 June 2021, following feedback from industry and to incorporate the new branding of the Critical Infrastructure Centre

Summary of any feedback or complaints

Engagement and feedback from industry has continued to be generally positive, as industry increasingly recognises the benefits of being able to access security related information from government, and guidance on implementing mitigations to protect critical business operations.

The Department has continued to work with 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

Supply chain risk assessment

As part of the TSSR notification obligations, the Department continued to encourage carriers to undertake a risk assessment of their vendors' equipment and services. The Department has identified a need to provide more guidance on the specifics of the supply chain risk assessment and is working towards publishing guidance materials.

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

5G Cloud compute

The Department notes that 5G cloud orchestration featured in a number of technical discussions with carriers over the last financial year. Through the discussion, the Department has attempted to balance the ideal availability construct provided through virtualised compute technologies against the threat to both the carriers' Core and emerging Edge use cases.

COVID-19 implications

The ongoing COVID-19 pandemic has created many challenges for industry to manage network performance to support a sizeable population to work or study remotely. The pandemic has brought about a rethink amongst carriers with respect to their own staff and vendors' staff working from home arrangements to support network operations. Some carriers also briefed the Department on how they are managing potential security risks where their vendors' staff were working from home at offshore locations. To assist industry through these trying times, the Department maintained ongoing dialogues with all major carriers and proactively engaged with smaller carriers to ensure they were being appropriately supported.

Managed service providers

The Department has seen an increase in the number of notifications involving managed service providers (MSPs), as well as an increase in the range and scope of functions that MSPs are proposing to undertake on behalf of customer carriers.

The Department received multiple notifications during the reporting period in which the CAC considered that a carrier's proposed use of an MSP could interfere with the carrier's ability to maintain competent supervision of, and effective control over, telecommunications networks and facilities owned or operated by the carrier, as required under section 313(1B). The CAC's concerns were most often associated with:

- inadequate proposed supervision by the carrier of the MSP's activities on the carrier's networks and facilities (including through over-reliance on self-supervision and self-reporting by the MSP)
- inadequate consideration by the carrier of the location(s) from which the MSP would be providing the services
- limited assurance that the carrier could demonstrate effective control over networks or facilities being serviced by the MSP.

In each of these instances during the reporting period the CAC informed the relevant carriers of the concerns and suggested measures that they could implement to ensure they could continue to comply with their security obligation while proceeding with the changes.

Network function virtualisation (NFV) and orchestration

Multiple carriers notified the CAC during the reporting period about changes involving network function virtualisation (NFV), frequently in combination with 'automated' network orchestration solutions. These changes featured high levels of technical complexity and equally complex supply chains.

In several instances the CAC had concerns about the notifying carrier's understanding and appreciation of the risks presented by the proposed change, particularly the risks associated with complex multi-vendor/subcontractor, multi-jurisdiction supply chains. The CAC also had concerns in several instances with carriers misunderstanding the level of exposure they had in proposing to outsource or 'hybridise' their infrastructure environment.

Again, in each of these instances during the reporting period the CAC informed the relevant carriers of the concerns and suggested measures that they could implement to ensure they could continue to comply with their security obligation while proceeding with the changes.

Mobile 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 has continued to work closely with telecommunications operators to ensure they understand their TSSR obligations with respect to deploying and operating 5G networks and services.

The Department continues to work with non-5G mobile network operators to understand and manage the potential sustainment risks associated with the United States' export restrictions affecting certain telecommunications infrastructure vendors.

Approach to the notification obligation

There is some variation among carriers in their approach to the TSSR notification obligation, as outlined in submission to the Parliamentary Joint Committee into Intelligence and Security's current review into the operation of TSSR. Most carriers the Department has interacted with under TSSR are engaging positively with their 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 have continued to work 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.

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.

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, providing advice to the extent possible, and advising the entity to submit a further notification once the project is more advanced.

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 requirement

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.