Australian Government

Critical Infrastructure Centre

Telecommunications Sector Security Reforms Administrative Guidelines

The Australian Government has prepared these Guidelines to assist members of Australia's telecommunications industry to understand their new obligations under the *Telecommunication Act 1997*, introduced by the *Telecommunications and Other Legislation Amendment Act 2017* (known as the Telecommunications Sector Security Reforms, TSSR).

Version 1.0 published 11 October 2018

Contents

Purpose of this guide

This document is designed to help the telecommunications industry understand the framework under the *Telecommunications Act 1997* (the Act) introduced by the *Telecommunication and Other Legislation Act 2017*, known as the Telecommunication Sector Security Reforms (TSSR), and assist them to understand their role in helping to protect critical infrastructure from national security threats.

Detailed guidance is provided to carriers, carriage service providers and carriage service intermediaries (C/CSPs) on how to comply with obligations to:

- do their best to protect telecommunication networks and facilities from risks of unauthorised interference or unauthorised access; and to
- notify Government of proposed changes to their telecommunications systems and services.

The Guidelines also detail the importance of the enhanced partnership between Government and the telecommunications industry and the processes to support early engagement on potential risks, increased information sharing on specific national security risks, and increase industry awareness of national security vulnerabilities and risks.

Due to the sensitive and fluid nature of national security threats, it is not possible to comprehensively outline all the threat sources and threat vectors and appropriate mitigations in this document. It is intended that security agencies will supplement the advice provided in this document with specific and general threat information on a case by case basis.

The Communications Access Co-ordinator (CAC) through the Critical Infrastructure Centre (the Centre) within the Department of Home Affairs is responsible for the administration of TSSR and for ongoing engagement with the telecommunications industry.

Who should read this document?

This document is intended to be read by senior management and executives, as well as employees in security and regulatory roles and technical officers responsible for telecommunication network design and maintenance in the telecommunications industry.

Disclaimer

This document is intended as a guide and readers should seek legal, technical and risk advice as to their own specific needs. The information in this document should not be relied upon as legal advice. The provision of this information does not override the need to observe laws, in particular requirements to protect personal information under Australian privacy law.

List of acronyms

ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ASIO	Australian Security Intelligence Organisation
ATT	Administrative Appeals Tribunal
BGLU	ASIO Business and Government Liaison Unit
BSS	Business Support Systems
CAC	Communications Access Co-ordinator
C/CSP	Carrier, carriage service provider or carriage service intermediary
CERT	Computer Emergency Response Team
C/NCSP	Carrier or nominated carriage service provider
CREST	Council of Registered Ethical Security Testers
CSG	TISN Communications Sector Group
CSI	Carriage service intermediary
CSP	Carriage service provider
DIO	Defence Intelligence Organisation
EPC	Evolved Packet Core
HLR/HSS	Home Location Register
IRAP	International Road Assessment Programme
ISO	International Organization for Standardization
NOC	Network Operations Centre
OAIC	Office of the Australian Information Commissioner
OSS	Operations Support Systems
OTT	Over the top
PSPF	Protective Security Policy Framework
SOC	Security Operations Centres
TISN	Trusted Information Sharing Network
TSSR	Telecommunication Sector Security Reforms
VMS	Voice Mail Systems

Critical Infrastructure Centre contacts and information

Further information about TSSR, approved forms and the secure *TSS submission form* are available on the Critical Infrastructure Centre website.

Any questions about this document or TSSR should be directed to Critical Infrastructure Centre by email at cicentre@homeaffairs.gov.au or by telephone on (02) 5127 7387.

Overview of the TSSR framework

The aim of TSSR is to encourage early engagement and collaboration between the Australian Government and the telecommunications industry to meet its security obligation by identifying and managing national security risks associated with proposed changes to telecommunications systems and telecommunications services.

Australia's telecommunication networks, systems and facilities are critical infrastructure that are vital to the social and economic well-being of the nation. National security threats including espionage, sabotage and foreign interference pose a real and growing threat to Australia's telecommunication infrastructure.

The TSSR framework responds to these threats by strengthening existing industry-government engagement and embedding a risk management approach by the telecommunications industry with the aim of raising the overall security posture of Australia's telecommunication sector.

The reforms require the telecommunications industry to take into account a broader range of security risk factors when making investment and operational decisions to protect broader national security interests.

The TSSR framework will also provide industry with greater certainty about what is expected of them to protect national security interests.

Who has obligations?

The TSSR obligations in the Act apply to all carriers, carriage service providers and carriage service intermediaries within the meaning of the Act:

- **Carriers** - entities who hold a carrier licence.
- **Carriage service providers** – entities that use a network unit to supply listed carriage services to the public.
- **Carriage service intermediaries** - entities that arrange the supply of a listed carriage service by a carriage service provider to a third person.
- **Nominated carriage service providers** – carriage service providers or carriage service intermediaries nominated under the *Telecommunications (Interception and Access) Act 1979*.

This includes carriers and carriage service providers ('providers') that have telecommunications networks ('networks') and facilities, based in Australia or overseas, which are used to provide services and carry and/or store information from Australian customers.

Global companies operating in Australia

To the extent networks, facilities and services are operated and managed in other countries, and do not have an Australian link, the TSSR requirements under the TSSR framework do not apply.

Over the top (OTT) service

To the extent an OTT provider is a carrier or carriage service provider, it will be obligated to protect its networks and facilities under the Act and comply with the security obligation. The OTT provider's obligation, however, would only extend as far as it has access to, or control of, networks and facilities.

Cloud computing

Cloud computing is reliant on telecommunications networks and facilities for its operation. Carriers, carriage service providers and carriage service intermediaries that use or offer cloud computing services or infrastructure are required to do their best to protect networks and facilities from unauthorised interference or unauthorised access, including ensuring the confidentiality of information' contained in the cloud' and the availability and integrity of networks and facilities.

If a company is unclear if it has obligations under the TSSR framework within the meaning of a carriage service provider or a carriage service intermediary, independent legal advice should be sought to clarify its responsibilities and potential security obligation under the Act.

Security obligation

Sections 313(1A) and (2A) of the Act require all **carriers, carriage service providers and carriage service intermediaries (C/CSPs)** to *do their best* to protect telecommunication networks and facilities owned, operated or used by them from unauthorised access or interference. This obligation requires C/CSPs to maintain competent supervision of, and effective control over, telecommunication networks and facilities owned, operated or used by the C/CSPs.

For further information see *Security obligation* on page 17.

Notification obligation

Section 314A of the Act requires all **carriers and nominated carriage service providers (C/NCSPs)** to notify the CAC of proposed changes to their telecommunication systems or services that are likely to have a *material adverse effect* on their capacity to comply with the security obligation.

The CAC will assess notifications of proposed change and may request further information about proposed changes and will engage with C/NCSPs to develop appropriate measures to reduce identified security risks. The notification requirement seeks to facilitate security considerations being embedded into business decision making and operations.

For details see *Notification obligation* on page 24.

Regulatory powers

The *Telecommunications and Other Legislation Amendment Act 2017* introduces new powers to direct C/CSPs to take specific action, or refrain from taking specific action, or provide information. These powers are intended to be used as a last resort.

Power to issue directions to C/CSPs

Section 315B of the Act enables the Minister for Home Affairs (the Minister) to issue a direction to a C/CSPs to do, or not do, a specified act or thing where there is a risk of unauthorised interference or access involving telecommunications networks or facilities and the risk would be prejudicial to security. These include risks to:

- the confidentiality of information contained on or carried across telecommunications networks and/or facilities;
- the availability and integrity of telecommunications networks and facilities and this was prejudicial to security

A direction can only be issued if the Australian Security Intelligence Organisation (ASIO) has issued an adverse security assessment in relation to the C/CSP and following reasonable steps to negotiate in good-faith with the C/CSP to achieve an outcome of eliminating or reducing the risk.

Information gathering power

Section 315C of the Act enables the Secretary of the Department of Home Affairs (or the Director-General of Security, ASIO if authorised), to request information or documents from a C/CSP for the purpose of assessing compliance with the security obligation.

Civil penalty regime in the Act

The Minister can initiate proceedings in the Federal Court to seek civil remedies for non-compliance with the security obligation, a direction and/or request for information, including civil penalties, enforceable undertakings and injunctions.

For details see *Regulatory powers* on page 30.

Information sharing and engagement

The TSSR framework is intended to formalise and strengthen existing engagement and information sharing practices between industry and Government.

General guidance and engagement

The TSSR framework will formalise the relationship between Government and C/CSPs to achieve more effective collaboration on the management of national security risks. The aim is to encourage early engagement on proposed changes to networks and services that could give rise to a national security risk and collaboration on the management of those risks. The regulatory objective is to achieve national security outcomes on a cooperative basis rather than through the formal exercise of regulatory powers.

A full list of security and information partners is under Appendix A.

Specific threat advice

Carriers and providers with a high risk profile will be expected to engage more regularly with security agencies. A natural trigger for this engagement will be when these carriers and providers notify the CAC of proposed changes to their telecommunications systems and services. Alternatively, security agencies may initiate contact if, for example, they become aware of a particular risk to a network or facility.

Security agencies will also seek to develop more collaborative partnerships with high risk profile C/CSPs to encourage an open dialogue about emerging threats and partnerships to manage these threats. The objective of closer engagement with this group is to foster greater collaboration.

Security agencies may seek to establish regular ongoing meetings with C/CSPs who they consider to be high risk to provide general and specific threat advice, discuss proposed changes to systems and services and collaborate to develop mitigations or security measures to address security risks. Existing forums such as the Trusted Information Sharing Network (TISN) may also be used to discuss threat advice and appropriate control measures.

Security agencies may request that specified personnel within a C/CSP apply for a security clearance. Having cleared staff will give security agencies the option of sharing classified information where there is a need to know this information. While these individuals cannot pass classified information to colleagues without security clearances, they will be able to provide better informed guidance on identifying and addressing network security risks.

If a C/CSP does not have security cleared staff, security agencies will still seek to engage with them and share what information they can about security risks.

Risk Profiles

From a security perspective, a high risk C/CSP is more likely to be actively targeted and exploited by state-based actors and organised criminals and therefore have an increased risk of espionage, sabotage or foreign interference.

Risk profiles are based on:

- **percentage of market share** - the larger the number of customers, the greater the aggregate data base;
- **sensitivity of customer base** - some customers will have more information of a more sensitive nature being communicated and held on networks and facilities than others - such as government and critical service

providers, science and research organisations, large or significant commercial organisations, and large healthcare provider organisations (or their suppliers and business partners); and

- **criticality of the network** - for example, where the telecommunications network or service supports the delivery of other critical services, e.g., health, power, water and/or where it provides niche services.

Case study – Engagement with a C/CSP to mitigate security risks

A high risk profile Australian Telecommunications Company was considering a proposal to introduce a new customer management and billing system. The CAC assessed management and billing systems as a sensitive part of a telecommunications system because they hold aggregate customer data and information. Through reporting from an overseas partner, the CAC became aware of security concerns associated with the company's preferred supplier. In particular, that the preferred supplier could facilitate foreign intelligence services gaining unauthorised access to sensitive customer and network information.

What engagement occurred?

The C/CSP advised the CAC early in the planning stage of the proposal enabling the CAC to advise the company of the potential national security risks associated with engaging the preferred supplier and the types of measures that could be implemented to manage the risks and provide an adequate level of mitigation.

The company acknowledged the potential national security risks and incorporated the measures and mitigations that the CAC identified. The CAC also suggested further risk mitigation options for consideration to improve the company's overall security posture and its capacity to comply with the security obligation.

What are the implications for this TSSR framework?

In this case the national security risks were managed through early engagement between the carrier and the CAC. TSSR seeks to support this cooperative approach through a more formal, transparent and accountable TSSR framework. Development of risk mitigation measures to respond to the identified security risks was a cooperative process allowing development of the most cost-effective and practical measures to mitigate the risk.

Operational assistance

Effective protection of telecommunications networks and facilities is not just about prevention of threats, it also relates to the overall resilience of an organisation. Monitoring processes to detect cyber-attacks and plans to respond to, and recover from, a cyber-attack are also important to consider. A key component of a response plan is knowing when to report a cyber-incident.

Further information about developing effective monitoring processes and response plans is available in the resources listed under Appendix C.

TSSR framework principles

Implementation of the TSSR framework by Government and industry in good faith

C/CSPs are expected to implement the security obligation and engage with Government co-operatively and in good faith. For example, C/NCSPs required to notify the CAC via the Centre's secure portal of changes to their telecommunication systems or services under section 314A of the Act will be expected to **provide sufficient information** about proposed changes in any notification to allow the CAC and security agencies to accurately assess any potential national security risks.

Government will also work with C/CSPs co-operatively to identify and mitigate risks to Australia's national security arising from the design, build or operation of telecommunications systems and networks. The Government recognises that mitigation measures to address some security risks to networks may have a cost impact on companies.

For this reason, the Government will work closely with C/CSPs to ensure that the TSSR framework operates in a pragmatic, practicable and cost-effective way for the telecommunications industry. Government agencies should have taken adequate steps to engage the C/CSP, listen to the C/CSP's concerns and work with the C/CSP to develop mitigation measures reasonably necessary for addressing the risk.

Key security principles

The TSSR framework is based on the following principles:

Protection of telecommunications infrastructure is a shared responsibility

Industry-government engagement and information sharing practices about security risks to systems and networks is the most practical way of managing national security risks, including espionage, sabotage and foreign interference.

Owners and operators of telecommunications networks and systems are primarily responsible for ensuring their security– this is a matter of good corporate governance and business continuity. Owners and operators are best placed to manage risks to their operations and determine the most appropriate strategies to boost resilience.

Even the most informed company, however, is unlikely to have access to the most up to date threat information that is available to security agencies. The Government is the primary source of security threat information and the CAC will work with the telecommunications industry by sharing threat advice and providing guidance about risk management.

A risk management approach

The Administrative Guidelines do not specify how telecommunications companies must protect their networks. Instead they encourage a risk-based approach to allow companies to choose the best technical and business solutions. There is no single solution to protect networks and facilities – good security is multi-layered and tailored to the identified threat.

Good risk management is an ongoing process. It involves establishing a context, determining threats, vulnerabilities and criticality of systems and information, then analysing likelihood and consequence before evaluating and applying risk controls to the identified vulnerability.

Key to any risk assessment is an appreciation of how a threat or vulnerability will affect the confidentiality of communication contained on and information carried networks and facilities, and the integrity or availability of networks and facilities.

Embedding security considerations into business processes

Well considered security measures integrated into business systems and processes from the start are ultimately more effective and less costly than security measures added on later. Good security is embedded as part of an organisation's principles, practices and plans – not implemented as an afterthought. If security is only considered at the end of product design, it can leave systems or business arrangements exposed and add an extra layer of cost and complexity.

For this reason, C/CSPs are encouraged to engage with the CAC early in the process of planning changes to systems and services which affect core and sensitive parts of a network and may give rise to national security risks.

C/CSPs are also encouraged to engage with the CAC at any stage if they are uncertain about what parts of a network or system may be vulnerable to unauthorised access or unauthorised interference.

A list of resources to assist C/CSPs to protect networks and information are listed at Appendix C of the guidelines.

National security risks

Telecommunications networks and facilities are attractive targets for espionage, sabotage and foreign interference activity by state and non-state actors

Telecommunication networks and facilities are critical infrastructure

The security and resilience of telecommunications infrastructure significantly affects Australia's social and economic well-being. Government and business are increasingly storing and communicating large amounts of information on and across telecommunications networks and facilities. For these reasons, the telecommunications networks and facilities of C/CSPs are attractive targets for espionage, sabotage and foreign interference activity by state and non-state actors.

In some cases, national security risks will overlap with general security risks related to the running of a business, for example ensuring personal information about customers are protected. The difference lies in how that risk may be exploited by specific threat actors, and the impact it may have on Australia's critical infrastructure.

In summary, national security risks relate to possible:

- compromise or degradation of telecommunications networks;
- compromise of valuable data or information of a sensitive nature, such as aggregate stores of personal data or commercial or other sensitive data;
- impairment of the availability or integrity of telecommunications networks; or
- potential impact on other critical infrastructure or Government services (such as banking/finance, health or transport services).

Global supply chains create particular challenges for implementing controls to mitigate personnel, physical and ICT security risks and therefore make networks and facilities more vulnerable to unauthorised access or unauthorised interference, such as espionage, sabotage, and foreign interference.

Vulnerabilities posed by outsourcing and offshoring arrangements

Carriers and providers can use third party cloud services and offshore service providers or facilities. The security obligation on carriers and providers remains whether they are using services or facilities offshore or within Australia.

A key area of interest for the Government is changes to networks and systems from outsourcing and offshoring arrangements that are managed by a vendor rather than the carrier or provider. Such outsourcing arrangements can provide a vendor with broad access to the carrier's or provider's networks, facilities and customer information and potentially heightens risks of unauthorised access or interference.

There may be a higher risk if the location from which these services and functions are to be performed offers the telecommunications operator limited visibility over the network or facility and therefore increased challenges for establishing and maintaining competent supervision and effective control.

Foreign solutions may operate in different legal environments which may present a number of potential national security risks and vulnerabilities, further exacerbated by an operator's lack of competent supervision and effective control in:

- the use of Cloud services and infrastructure, and where they are located;

- equipment running out of a foreign country and integrated back into the main network of an operator in Australia;
- staff recruitments (including staff vetting processes) where these processes may not align with Australian requirements, noting that staff may also not share a sense of corporate loyalty to the operator;
- the procurement and management of third party equipment vendors; and
- a solution being run under a vendor's security policy, which may not align with Australian legislation, best practice and/or existing compliance requirements or with the operator's own risk profile.

The objective of the TSSR framework is to ensure that these types of risks are appropriately identified and adequately managed by C/CSPs, industry and Government.

The TSSR framework is designed to ensure adequate risk management, not prescribe particular business models or service delivery solutions.

Core and sensitive network and facilities

Some parts of networks and facilities are generally considered to be core or sensitive and at a greater risk of intrusion or interference than other parts because they either store or carry sensitive personal, government or commercial communications and information (e.g. billing systems and lawful interception systems), or because they affect the availability and integrity of the network (e.g. operations support systems).

Proposed changes that are *likely to have a material adverse effect* on the C/NCSP's capacity to comply with its security obligation, for example changes in relation to maintaining operation, oversight, effective control, and competent supervision of the more sensitive parts of C/NCSP's networks and facilities require a notification to the CAC.

Network Operations Centres

A Network Operations Centre (NOC) or Security Operations Centre (SOC) contains the function or functions through which network operations are controlled, either as a function distributed among business units, or as a discrete business unit itself. This includes equipment, services, locations and processes used to support the network should this occur outside a NOC. This includes SOCs if distinct from the NOC (since they also perform key functions of network governance and oversight).

Lawful interception equipment or operations

Lawful interception equipment refers to any equipment, parts of equipment, or software designed to facilitate the lawful interception of communications on a network, which is permanently installed on the network, or able to be installed on request. For the purposes of this guidance, this also includes hardware or software which supports or facilitates this function.

Parts of networks that manage or store an aggregate of information

These are the places where information of a sensitive nature is likely to be stored, making the systems hardware and its support/operation of specific security interest. This refers to:

- databases which store data in bulk, such as call records or network traffic data,
- Operations Support Systems (OSS), or Business Support Systems (BSS) and other forms of business customer databases,
- proposals affecting the equipment or systems which interact directly and modify the network,
- areas of the network which store authentication credentials & encryption keys,

- Evolved Packet Core (EPC) and the Home Location Register (HLR/HSS) in mobile networks and
- places where privileged user credentials regarding the network and support systems themselves are stored and audit and oversight controls are retained.

Locations where traffic belonging to customers or end users is aggregated in large volumes, either in transit or at rest

Areas where data aggregates may include:

- points of interconnection or intersection with other networks, and other areas over which a significant proportion of the traffic on the network travels, in each case where the volume of traffic is, in absolute terms, 15% or greater of the total traffic travelling over the network, and
- large databases which reside in the core of the network and customer Voice Mail Systems (VMS), large email or message systems.

Case study – Consequences from the compromise of a 'sensitive part' of the network

Hackers in Greece infiltrated core components of the largest carrier in Greece's network to intercept mobile phone conversations. Rogue software was illegally implanted in four of the company's switches (the computer-controlled component of a phone network that connects two telephone lines to complete a telephone call). This created two parallel streams – one stream went to the correct recipient and the other to other stream to the hacker's network. This allowed hackers to listen in on conversations, potentially record conversations, and track the locations of key dignitaries as well as members of other political and non-political groups. As switches are at the heart of a telecommunications network, the hackers only needed to take over a few switches to carry out the attack.

What were the consequences?

It is not known who the hackers were (including whether trusted insiders were involved or whether it was an external attack) or what conversations were intercepted and the purpose of the interception. However, the list of targets was discovered. It included the phones of the Greek Prime Minister and other high-ranking ministers, government and military officials involved in sensitive political and business discussions.

How is this case study relevant to the TSSR framework?

This case study highlights why the TSSR framework is focussed on the sensitive parts of networks – the consequences of a compromise of these parts can be particularly serious.

In addition, this particular carrier had inadequate monitoring processes and controls to detect the unauthorised access to its lawful interception system. Under TSSR, C/CSPs will need to identify vulnerabilities in their networks and implement appropriate measures and controls to manage those risks.

Security obligation

The telecommunications industry must do their best to protect their networks and facilities from unauthorised interference or unauthorised access

Overview of the security obligation to protect networks and facilities

The national security obligation in Section 313(1A) of the Act has two elements - **C/CSPs** must *do their best* to protect their networks and facilities from unauthorised access or unauthorised interference to ensure the:

- confidentiality of communication carried on and information contained on telecommunications networks or facilities; and
- availability and integrity of telecommunications networks and facilities.

This will require C/CSPs to maintain **competent supervision** of, and **effective control** over, telecommunications networks and facilities owned or operated by the carrier or provider. What is required in a particular circumstance to secure a network or facility will differ depending on the risk factors of that network or facility and the risk profile of the C/CSP.

Unauthorised access or unauthorised interference

The obligation to protect networks and facilities from unauthorised access or unauthorised interference requires C/CSPs to maintain competent supervision and effective control may include taking reasonable steps to prevent intrusions or breaches within networks or facilities or to minimise the effect of malicious activity, demonstrable by the security controls in place. This will be particularly relevant where activity, if left unchecked, could provide opportunity to compromise the confidentiality, availability or integrity of telecommunications infrastructure or information carried by, or across it.

Risks to be mitigated include physical, personnel and systems. It is not reasonable or appropriate to give all personnel or contractors unfettered access to all parts of a network or facilities or information carried on it. Physical and logical controls need to be implemented along with clear access policies and the ability to track unauthorised access.

The term ‘unauthorised access’ should also be understood in line with its meaning within the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs). APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information; APP 11.1 requires an entity to take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. As such, APP 11 must be considered to the extent that communications and information carried or contained on telecommunications networks or facilities involves personal information. Although not defined within the Privacy Act itself, the Office of the Australian Information Commissioner (OAIC) has defined unauthorised access to be when personal information is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity or independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Case study - Unauthorised access resulting from failure to maintain competent supervision and effective control

A CSP operating in Australia contracted a webhosting business also located in Australia to hold the CSP's information about business clients, including details to verify the customers identities and details to provide a quoting and billing system.

The hacking group Anonymous was able to exploit vulnerability in an application used by the webhosting business to gain access to the data they held. Although the webhosting business kept the application patched, they had not upgraded to newer versions as they considered it the responsibility of the CSP (the version being used was seven years old). New versions had security features that may have prevented the attack by Anonymous.

Who was responsible for the breach?

The Office of the Information Commissioner (OAIC) found that the CSP had breached their obligation under the *Privacy Act 1988* to take reasonable steps to secure the personal information it held. The OAIC took the view that the CSP 'held' the information for the purposes of the Privacy Act, despite the fact that it was technically on the servers of a third party company.

What steps could prevent a breach such as this?

The OAIC recommended that the CSP:

- conduct regular reviews of all IT applications held internally or with external providers to ensure visibility to the CSP
- take steps to ensure all IT applications held internally or externally which hold or use personal information are subject to vulnerability assessment and testing, regular vulnerability scanning and have effective lifecycle management
- clearly allocate responsibility for lifecycle management of applications
- conduct regular audits of the CSP's IT security framework to ensure that security measures are working effectively, and that policies and procedures relating to data security are being complied with
- undertake further training for IT staff and relevant business units to increase their understanding of their data security obligations (including lifecycle management of IT applications), data security risks and threats, and the importance of following the CSP's policies and procedures that relate to data security
- undertake steps to ensure appropriate classification of data it holds either internally or externally, including whether it includes personal information and the sensitivity of that information
- review the terms of the contracts it has with IT suppliers that hold or manage the CSP's data to ensure clarity around which party has responsibility for identifying and addressing data security issues (such as vulnerabilities associated with old versions of IT applications).

How is the case study relevant to the TSSR framework?

The recommendations are relevant to any outsourcing arrangements to supply or manage equipment or services (not just hosting data). For example, if management of core parts of networks are outsourced without adequate security requirements these parts could be used to gain access to the networks.

Availability and integrity of telecommunications networks and facilities

Availability is about ensuring that authorised users have access to information, communications and telecommunications networks and facilities when required. An example where networks and facilities are not available would be a denial-of-service attack which prevents the ordinary functioning of the service, which could have serious economic, social or other consequences (particularly in an emergency).

Integrity relates to the accuracy and completeness of information and communications, as well as the protection of telecommunications networks and facilities from compromise or unauthorised modification. An example of a breach of integrity would be where a C/CSP's systems are accessed by a third party and modified to allow remote access by that party.

Confidentiality of communications and information

The security obligation under section 313(1A) has as its objective the protection of all communications carried on and information contained on networks and facilities, including information about the network itself, not just personal information.[1] In particular, the confidentiality of categories of information that are sensitive and vulnerable to unauthorised access or interference include government and business information such as intellectual property, information that could provide a competitive advantage, and information of a sensitive nature about a C/CSP's network, service delivery models and customers.

For example, a C/CSP that provides services to large businesses or research organisations (such as universities) may be at a greater risk of espionage, sabotage or foreign interference because of the commercial value of the information held by their clients (such as scientific research).

Type of controls

There are a number of controls which may assist C/CSPs to maintain confidentiality, including implementing robust access controls to limit who has access to communications and information. For example, access should be restricted to those who are expressly authorised to have access and who require access to do their job (i.e. provide access on a 'need to know' basis).

Access controls are particularly important for more sensitive parts of networks, in order to mitigate the threat of unauthorised access or interference from an insider (a trusted insider is a person such as an employee, contractor or business partner who uses insider knowledge or access to commit a malicious act to cause harm).[2]

The requirement to protect the confidentiality of communications and information relates to both information in transit and information being stored on telecommunications networks and facilities. Some storage solutions may present increased risk of unauthorised access or interference.

Encryption is important in many circumstances to ensure that information is stored and transmitted in a form that cannot be easily accessed by unauthorised individuals or entities. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted copy of your encrypted information.

[1] C/CSPs are already required to comply with the obligations contained in the Australian Privacy Principles (APPs) in Schedule 1 of the *Privacy Act 1988* which regulate the handling of personal information.

[2] Further information is available in Managing the insider threat to your business: A personnel security handbook, which is available from www.protectivesecurity.gov.au

Privacy regulations

Existing Australian legislation which sets out confidentiality and privacy obligations will also support compliance with the TSSR framework's security obligation. The following guidance materials issued by the Office of the Australian Information Commissioner (OAIC) may assist you to identify practical measures you can implement to secure all categories of personal information:

- Australian Privacy Principles Guidelines[3]
- Guide to securing personal information[4]
- Data breach notification — A guide to handling personal information security breaches [5]
- Privacy business resource 8: Sending personal information overseas[6]
- Privacy business resource 9: Ten tips to protect your customers' personal information[7]
- Privacy business resource 11: Telecommunications service providers' obligations arising under the Privacy Act 1988 as a result of Part 5-1A of the Telecommunications (Interception and Access) Act 1979[8]

The Australian Communications Media Authority has also published privacy guidance. These are the Better practice privacy tips for service providers.[9]

Case study – Implementation of related legislative obligations by a hypothetical company Security First Telco

An Australian carrier Security First Telco enters into a commercial outsourcing arrangement where another company will provide the network management functions, including supporting critical network elements of the telecommunications company's infrastructure where all network traffic is routed.

Additionally, the company has recently put measures in place to meet data retention obligations, including controls to protect access to stored customer information and traffic data. However, controls are not in place to protect the outsourced company having access to key network transit points where traffic logs can be generated and exported.

To comply with the security obligation under the TSSR framework to do their best to prevent unauthorised access or interference to ensure the confidentiality of communications carried on and information contained on networks and facilities, the carrier must also protect communications and information in transit and in use.

How do you meet your security obligation?

The most effective way for C/CSPs to comply with their security obligation is to:

- adopt a **risk-based approach** to protecting networks and facilities; and
- demonstrate **competent supervision** of, and **effective control** over, telecommunications networks and facilities owned or operated by the carrier or provider.

[3] www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/

[4] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information

[5] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

[6] www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-8

[7] www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-9

[8] www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-11

[9] www.acma.gov.au/theACMA/better-practice-privacy-tips-for-service-providers

Implement a risk management approach

Risk management includes the principle, processes and structures that underpin the effective management of potential opportunities and adverse effects. It is a structured approach to identifying, assessing and controlling risks that emerge during a program or project life cycle.

A risk-management approach under the TSSR framework should particularly focus on risks posed by arrangements with suppliers (in particular managed service providers) and particular service delivery models (i.e. outsourcing/offshoring) as these arrangements can expose the C/CSP to levels of risk that are more difficult to manage.

For example, if a C/CSP is using a supplier or managed service arrangement, or has outsourced elements of its enterprise such as data hosting, the C/CSP will need to consider the controls it has in place, or is proposing to put in place, to manage who can access and control sensitive parts of the network.

If a C/CSP is engaged in offshore arrangements, one of the key risks it would be expected to consider is the legislative environment in the particular country and whether offshoring particular parts of their business may mean that personal information about Australians, as well as sensitive commercial information or communications, may have to be provided to a foreign government under a lawful request in the foreign jurisdiction.

Industry should refer to the key documents listed below available from *International Organization for Standardization* (ISO)[10] for assistance in risk management and control mitigation for telecommunications:

- AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security, management systems—Requirements
- AS ISO/IEC 27002:2015 Information technology - Security techniques - Code of practice for information security controls

Case Study - Telstra's 'five knows of cybersecurity' to help assess risk[11]

The following five areas form a key part of Telstra's approach to information protection:

- Know the value of your data.
- Know who has access to your data.
- Know where your data is located.
- Know who is protecting your data.
- Know how well your data is protected.

Accurate assessment of risks to telecommunications networks and facilities, as well as the best mitigation strategies, rely on a comprehensive understanding of your business. Understanding these critical aspects of your business is a good first step for a C/CSP to develop an effective risk management approach to protecting data.

Demonstrate competent supervision and effective control

A key element in complying with the security obligation is ensuring that, regardless of any outsourcing and offshoring solution, a C/CSP is able to demonstrate that it has *competent supervision* and *effective control* of its network and facilities. In other words the C/CSP must demonstrate that it has processes, controls and arrangements in place to manage 'who and how' systems, networks and communications can be accessed.

[10] https://www.iso.org/isoiec-27001-information-security.html

[11] This case study has been included with the permission of Telstra. It is intended as an example only and may not be appropriate in all cases. Use of this methodology would not, on its own, be sufficient to meet legislative obligations under the TSSR framework

Competent supervision

Competent supervision refers to the capacity of a C/CSP to maintain proficient oversight of its networks, data and facilities. Competent supervision may be achieved either in-house or by using an independent third party. Competent supervision could include arrangements to maintain:

- visibility of network and facility operations;
- visibility of data flow and locations;
- awareness of parties with access to network infrastructure; and
- the capacity to detect security breaches or compromises.

External assessments provide a mechanism for organisations to have their security controls independently reviewed. The Information Security Registered Assessors Program (IRAP)[12] is governed and administered by the Australian Government Australian Signals Directorate (ASD). Australian organisations can engage an IRAP Assessor to conduct independent ICT assessments to ensure security compliance, identify security risks facing their organisation and develop mitigation strategies.

Penetration or vulnerability testing is another option to assess the vulnerability of a service to unauthorised access or interference. It is important that any penetration test considers both technology and human interaction. You may want to consider using a Council of Registered Ethical Security Testers (CREST) Australia[13] approved company when hiring a penetration tester. The companies that CREST certified individuals work for have subjected themselves to audit and scrutiny by CREST Australia, and have signed up to the CREST code of conduct.

Effective control

Effective control refers to a C/CSP's capacity to maintain direct authority and/or contractual arrangements to ensure that its network and facilities, infrastructure and information stored or transmitted, is protected from unauthorised interference or access. This would include authority over all parties with access to network infrastructure and the capacity to control who has access to network systems, facilities, information and access restrictions. Mechanisms to achieve this include:

- direct actions to ensure the integrity of network operations and the security of information they carry;
- terminate contracts without penalty where there has been a security breach or data breach reasonably attributable to the contracted services or equipment;
- address issues of data sovereignty;
- direct contractors to carry out mitigation or remedial actions ;
- oblige contractors to monitor and report breaches to the C/CSP; and
- re-establish the integrity of data or systems where unauthorised interference or unauthorised access has occurred (for example to confirm accuracy of information or data holdings).

Third party assurance may also mean implementing controls which can be tested, and, when fully effective, provide evidence that primary information security requirements have been, or are able to be, satisfied. The Protective Security Policy Framework (PSPF) administered by the Attorney-General's Department provides best practice guidance, in particular INFOSEC-4 and INFOSEC-5.

[12] Further information is available at www.asd.gov.au/infosec/irap/index.htm

[13] Further information is available at http://crestaustralia.org/

Case Study - security considerations for using Software as a Service applications

Security First Telco's (a fictitious company) employees have been asking their IT Department if they can use Software as a Service (SaaS) applications from a new provider. SaaS is the capability for a consumer to use a provider's applications running on cloud infrastructure or a cloud based infrastructure.

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Use of SaaS applications by Security First Telco's employees would be a form of 'shadow IT', a term used to describe hardware or software that is not supported by the company's central IT department.

Security First Telco knows there can be benefits from SaaS applications - it can be a cost effective way to provide software (as it does not require upfront investments and subscriptions can be adjusted from month to month). However, Security First Telco knows there can be risks. These include:

- Offshore storage of information - which means that the provider is subject to the laws of another country (which could include requirements to provide data about Security First Telco's Australian customers to another country's Government).
- Lack of visibility into the policies and processes of the provider - for example whether they comply with Australian privacy law and implement standard security controls.

For this reason, Security First Telco is going to consider the following matters when deciding whether to allow use of SaaS applications:

- Should all types of information be stored on SaaS applications?
- Will Security First Telco have visibility over the security processes used by the provider?
- Can Security First Telco verify whether the provider complies with Australian privacy laws and standard security controls?
- Will Security First Telco have visibility over the actions and processes of the provider?
- Will Security First Telco have the ability to require the provider to put in place certain protections (e.g. whether the contract specifies security requirements)?

Does the security obligation apply to existing systems?

C/CSPs are not expected to retrofit all systems on commencement of the security obligation, except in very rare cases where a significant security vulnerability is found in an existing network that could facilitate acts of espionage, sabotage and foreign interference.

In such cases, government agencies will seek to work with the C/CSP to develop cost effective solutions to better manage the risks posed by the existing vulnerability.

Notification requirements

The notification requirement seeks to facilitate a structure where national security considerations are embedded into business decision making and operations.

Overview of the notification obligation

The notification requirement in section 314A of the Act requires all carriers and nominated carriage service providers **(C/NCSPs)** to notify the CAC of planned changes to telecommunications services and systems if they become aware that a proposed change is *likely to have a material adverse effect* on their capacity to meet the security obligation.

A **material adverse effect** includes any change which could have an actual or potential negative impact on the capacity of the C/NCSP to comply with their security obligation to protect network and facilities from unauthorised access or interference.

For the purpose of compliance, any changes to core or sensitive systems or services (outlined on page 15) is likely to have a material adverse effect on the capacity of C/NCSPs to comply with their security obligation and will require a notification.

The notification requirement formalises information sharing between C/NCSPs and the government and is triggered at the time of planning proposed changes to networks and services, rather than following implementation. Although the legislation does not specify when a C/NCSP should notify government of changes, it is in the C/NCSP's best interests to notify of a proposed change as early as possible in the design and planning stage and prior to finalising arrangements to implement the change. For example, the stage at which a detailed business case is being prepared for the company Board for decision might provide a guide for the appropriate time in the planning process for notifying the CAC.

In the event a C/NCSP deems a change is *unlikely* to have a material adverse effect on its capacity to meet the security obligation, it is expected that the C/NCSP maintains a record of the decision not to provide the CAC with a notification. The CAC may, during routine compliance activities, seek evidence regarding how the C/NCSP determined the change did not have a material adverse effect.

Accordingly, C/NCSPs should engage regularly with existing information sharing forums (see *Information sharing* and *Engagement* on page 10) and other relevant security advice forums (outlined at Appendix C) to maintain their awareness of the security threat environment.

Notifiable changes

This section explains the kinds of proposed changes that the CAC will need to be notified of. This summary is illustrative and not exhaustive. It will change over time to reflect changes in the security threat environment, technology and telecommunications infrastructure and methods for delivering telecommunications services.

The legislation limits the scope of the notification requirement to changes that are *likely to have a material adverse effect* on the capacity of the C/NCSPs to comply with their security obligation. The requirement to notify arises only from a *change* to a system or service, not from existing operations.

Section 314A of the Act outlines the types of changes in arrangements that will likely require a C/NCSP to notify the CAC:

- providing new telecommunications services, for example VoIP, email and messaging services;
- changing the location of telecommunications equipment and network management equipment (including moving equipment outside Australia);

- procuring telecommunications equipment and network management equipment (including procuring equipment that is located outside Australia) where the equipment forms or supports 'sensitive parts of networks';
- entering into outsourcing arrangements:
  - to have all or part of the telecommunication services provided for a C/NCSP, or
  - to have all or part of the provision of telecommunication services managed for a C/NCSP, such as managed services, or
  - for the management of all or some of C/NCSP's telecommunications data.
- a C/NCSP entering into arrangements to have all or some of its telecommunications information accessed by persons outside Australia;
- a C/NCSP entering into arrangements to have all or some information or documents to which subsection 187A(1) of the *Telecommunications (Interception and Access) Act 1979* applies kept outside Australia;
- changing the levels of access to, or control of, sensitive data or information, including customer data; and
- changing the management of services, including new contractual arrangements and third parties.

It should be noted that C/NCSPs can submit a single (rather than repeated) notification for a standard build or a bulk change.

Standard build notifications

A standard build may comprise consistently procured equipment build or a network addition, which is replicated throughout the network. Notification of the standard build is only required in the first instance, provided the build does not change to a type of equipment that has not been previously submitted to the CAC by that network operator. In instances where a standard build is used, notification should also include details of the geographic locations in which it is intended to be deployed.

Should the standard build change from that notified, a new notification would need to be submitted outlining the changes in the new build.

Bulk change notifications

One notification may be submitted for a standard set of equipment to be used in a network proposal, i.e. a bulk change. This could include all versions of a certain type of networking equipment, and the software/firmware builds that are likely to be deployed on it.

Notification could also be supplied for a specific product range which may change incremental versions over time. Once the CAC has considered the proposal covering the product range, the equipment would be able to be deployed on the network without the need to submit a new notification.

For example, where security agencies have been previously engaged on a similar change to a network or have previously approved a proposed procurement process, architecture or equipment it may not be necessary to submit a notification for the same type of change.

There are, however, some practical limitations to notifications of bulk changes. A notification with an excessive number of equipment types or for an entire vendor’s product range does not amount to notification of a bulk change.

Notifiable equipment

Notifiable equipment includes equipment that is essential to the C/NCSP’s telecommunications system or the provision of its services. Any equipment that manages information within the meaning of section 276 of the Act is also notifiable equipment.

Changes not likely to have a material adverse effect

C/NCSPs providers do not need to submit notifications for changes that do not affect their capacity to comply with their security obligation. Examples include:

- replacing like-for-like equipment
- day-to-day changes, such as routing changes or software updates;
- emergency changes, including urgent changes to maintain the availability of a network, provided you submit a notification as soon as practicable; and

  testing or trials not connected to an Australian telecommunications network and where protections are applied to customer data.

Case Study – Which proposed changes to their systems should the hypothetical company Security First Telco notify to Government?

Security First Telco is reviewing proposed changes to their telecommunications systems to decide which changes need to be notified to Government.

Examples of changes that should be notified

After a risk assessment of options (based on the guidance in this document), they have decided the following changes are *likely to have a material adverse effect* on their capacity to protect their networks from unauthorised access and interference (i.e. espionage, sabotage and interference) for the following reasons:

Engagement of a new billing provider

This proposal would likely involve the new billing supplier and a third party, being used by the billing supplier, having access to Security First Telco's sensitive customer information during the projects and possibly after the project as part of support arrangements.

After discussing the project with Government, appropriate risk mitigation could include controlling the access any third party company located outside of Australia may have to the personal information and billing data for all of Security First Telco's Australian customers.

A mobile network operator to deploy Long Term Evolution (LTE) technology

A mobile network operator plan to deploy LTE would likely mean new or upgraded equipment and involve an equipment supplier or managed service provider to have access to sensitive parts of Security First Telco's networks, including access to communications.

In this instance, appropriate mitigation could include ensuring adequate control and monitoring over levels of access the equipment supplier may have, including remote access arrangements. This would also apply if the network operator were planning to trial new equipment before considering any tender related activity.

Engagement of an existing supplier to upgrade core routing equipment

This plan would likely require a supplier to access or install software on equipment where a significant proportion of the network traffic travels including telecommunications intercepted traffic. Appropriate mitigation could address concerns related to unauthorised access to the network real time traffic or interception data.

Renewal of a contract not previously notified to Government

Security First Telco entered into a contract with a company to manage their data storage solution (which includes all customer details) before they were obliged to notify Government of changes to systems under the TSSR framework. Although the new contract would reaffirm the status quo, Security First Telco should notify Government that they are planning to renew the contract with this supplier as this arrangement could affect the ability of Security First Telco to maintain effective control and competent supervision of its networks and services.

In most cases, if security agencies have not already identified the current arrangement as potentially exposing the network to security vulnerability it will likely be assessed and confirmed as not giving rise to security risks. However there may be incidents where security agencies can provide guidance and advice to enhance control and supervision of data stored by the vendor.

As noted, C/CSPs are not expected to retrofit all systems on commencement of this security obligation, although a renewal of a contract may provide an opportunity to better mitigate any existing security vulnerabilities (for example, specification of mandatory security requirements in the contract itself).

Examples of changes not required to be notified

Through their risk assessment, Security First Telco has assessed that the following changes are not likely to have a material adverse effect on their capacity to protect their network and therefore do not need to be notified:

Renewal of a contract previously notified to the Government

Security First Telco advised the CAC when they first engaged this supplier to provide their data storage solution. However, given the CAC previously advised there were no security concerns with this supplier (because Security First Telco had built in security requirements and protections into the original contract) there would generally be no need to notify again as there would be no change to existing arrangements (i.e. there are no changes to the location of the data storage or contractual requirements). However, if the threat environment has changed (for example if Security First Telco has been advised by security agencies of new security threats) then Security First Telco may need to notify of the renewal of a contract.

Construction of new mobile towers by Security First Telco

Security First Telco has assessed that proposed construction of further mobile towers is unlikely to have a material adverse effect on their capacity to protect their networks from unauthorised access and interference because they are using a standard build, which has been previously notified to the CAC and assessed as not giving rise to security concerns (see page 25 for further information about standard builds).

Upgrades to the operations centre

Security First Telco is expanding and renovating their operations centre in Australia, including new access restrictions. As there will be no substantial change to existing arrangements (in fact the new access restrictions are likely to tighten physical and logical access and therefore will enhance the company's capacity to protect their network from security risks) there is no need to notify of the changes.

Business-as-usual maintenance

Security First Telco does not need to notify of ongoing maintenance of legacy systems and infrastructure which do not amount to substantial modifications in network design, operations and service delivery.

Administrative process for notifications

This section explains the steps for C/NCSPs to submit a notification and the administrative processes the CAC will undertake to assess notifications. A notification process chart is at Appendix B of the guidelines.

Notification and notification exemption applications must be made using the approved **Notification form (TSS1)** or **Notification Exemption form (TSS2)** available on the Critical Infrastructure Centre website.

Please check that all required questions are answered and that the form is dated and electronically signed and submit the PDF notification and all attachments through the Centre's secure submission portal.

An automatic receipt will be generated when the notification has been successfully submitted to the CAC showing the time and date of submission.

Following the submission of a *complete* notification, a C/NCSP will receive one of the following notices from the CAC **within 30 days** of notifying of a proposed change:

- **Further information:** request under subsection 314B(1) for further information about the planned change so the Centre can assess whether there is a risk of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security
- **Risk associated:** notice under subsection 314B(3) advising the C/NCSP of a risk associated with the planned change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.

  In this situation the Centre will seek to engage the C/NCSP to discuss and determine appropriate measures to reduce or eliminate the risk of interference or unauthorised access.
- **No risk:** notice under subsection 314B(5) advising that the CAC is satisfied there is not a risk from the planned change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.

While the above process is premised on cooperative engagement and collaboration, in the event that a C/NCSP refuses to provide information requested by the CAC or fails to address potential security risks, the responsible Minister may exercise a direction or information gathering power.

Notification exemptions

C/NCSPs may receive **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), either on the CAC's own initiative or a C/NCSPs can submit a written application to the CAC using the **notification exemption form (TSS2)**.

If a C/NCSP 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 C/NCSP may apply to the Administrative Appeals Tribunal (AAT) for review of a decision by the CAC not to grant an exemption.

A **full exemption** means the C/NCSP does not have to notify the CAC of any planned changes to telecommunications systems or services, whereas a **partial exemption** may be given in relation to certain categories of changes or in respect of particular parts of the C/NCSP's business.

For example, a large carrier which offers a number of different types of services, may be exempted from providing any notifications in relation to a part of their business (for example, a subscription television service), but would still be required to notify of changes to other parts of their business. The details of a partial exemption would be specified in a notice provided to the C/NCSP.

The CAC may also grant **class exemptions** on their own initiative. Class exemptions will typically relate to particular classes of low risk service or network operator.

Grounds for exemption

The CAC will consider applications for exemptions on a case-by-case basis, with regard to the security risk profile of a company based on factors such as:

- percentage of market share
- sensitivity of customer base
- criticality of network.

The CAC will not grant unnecessary exemptions; for example, in the instance that a carrier or nominated carriage service provider does not have obligations to notify for a particular change.

Security capability plans

A security capability plan may be submitted each year to notify about all proposed changes that are *likely to have a material adverse effect* on their capacity to meet their security obligation to protect networks, instead of notifying the CAC of each individual change to systems and services – see section 314C of the Act. In essence the security capability plan is a bundle of individual notifications.

What proposed changes should be included in a security capability plans?

Security capability plans should only include changes that are *likely to have a material adverse effect* on the capacity of the C/NCSP to comply with their obligation to protect their networks and facilities from unauthorised access or interference under subsections 313(1A) and (2A) of the Act.

A C/NCSP may only submit one security capability plan in a 12 month period; if a C/NCSP wants to notify about any additional changes then an individual notification must be completed.

How far in advance security capability should plans forecast?

While the legislation does not prescribe how far in advance the plan should capture proposed changes the CAC has a maximum of 60 days to consider notifications covered in the plan. Accordingly, it may not be feasible to include changes that have tight deadlines for implementation and which require CAC consideration in a shorter timeframe to avoid delaying a project. For such proposed changes, a C/NCSP may wish to complete a standard notification form which the CAC must respond to within 30 days (unless further information is required).

What other information can be included in a security capability plan?

C/NCSPs may like to include information about their practices, policies or strategies in place to secure their networks from unauthorised access and unauthorised interference. For example, this might include:

- a description of the risk assessment processes used to identify and manage security risks on networks, systems and services;
- arrangements and mechanisms in place for overseeing contracted managed service provider compliance with security requirements etc. (for example standard contract terms concerning personnel, logical and physical security requirements and access restriction and how compliance is monitored and enforced); and
- assurance processes for vetting security practices of a vendor.

C/NCSPs should also detail any current or proposed mitigation measures or controls to reduce the risk of unauthorised access or interference. This approach could facilitate more targeted engagement between the C/NCSP and government on the C/NCSP's approach to meet its security obligation and better assist the CAC during the assessment process associated with each proposed change.

Regulatory powers

Enforcement mechanisms are intended as a last resort to address non-cooperative conduct rather than to penalise action and decisions taken in good faith.

Direction to specify an action

The Act provides that the Minister may make the directions to a C/CSP under the following circumstances:

- if the use or supply of a carriage service is prejudicial to security (under s 315A); or
- if there is a risk of unauthorised interference or access involving networks of facilities (s 315B).

Section 315A provides that the Minister may issue a direction not to use or supply, or to cease using or supplying a carriage service if:

- a person who is a C/CSP uses or supplies, or proposes to use or supply, for the person's own benefit, one or more carriage services; and
- the Minister, after consulting with the Prime Minister, considers the proposed use or supply would be prejudicial to security.

The direction must relate to a carriage service generally and cannot be expressed as applying to the supply of a carriage service to a particular person or class or persons.

Section 315B of the Act enables the Minister to issue a direction to the C/CSP to 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. These include risks to the:

- **confidentiality of information** contained on or carried across telecommunications networks and/or facilities;
- **availability and integrity** of telecommunications networks and facilities and this was prejudicial to security.

Noting the TSSR framework is premised on cooperative engagement and collaboration, the Minister's power under s 315B is intended as a last resort to achieve compliance.

Transparency and accountability measures

The Minister may only issue a direction to a C/CSPs if:

- the Minister is satisfied that there is a risk of unauthorised interference with or unauthorised access to networks or facilities that would be prejudicial to security having reference to the meaning of 'security' in the *Australian Security Intelligence Organisation Act 1979*; and
- ASIO has made an adverse security assessment in respect of a C/CSP.

In addition, the Minister may only issue a direction under s 315B if satisfied that all reasonable steps have been taken to negotiate, in good faith, with the C/CSP to achieve an outcome of eliminating or reducing the security risk.

Before giving this direction, the Minister must also consider a range of other matters including, but not limited to:

- an adverse security assessment by ASIO;
- the costs, in complying with any direction, that would be likely to be incurred by the C/CSP; and
- the potential consequences that any direction may have on competition in the telecommunications industry, as well as customers of the C/CSP.

The requirement to have regard to these matters are intended to ensure that a direction is proportionate and reasonable and does not have an unnecessary negative effect on the C/CSP's business or impede market innovation and competition.

Consultation

Before giving a C/CSP either direction the Minister must provide a copy of the written notice to the Australian Communications and Media Authority (ACMA).

Where the Minister issues a s 315B direction, the Minister must:

- consult with the Minister administering the Act; and
- provide the C/CSP with a written notice setting out the proposed direction and invite the C/CSP to make written representations to the Minister in relation to the proposed direction, and have regard to any representations made.

The Act does not limit the persons with whom the Minister may consult.

Administrative Appeals Tribunal

In accordance with the accountability provisions contained within Part IV of the *Australian Security Intelligence Organisations Act* 1979 (ASIO Act), a C/CSP can seek merits review of the ASIO security assessment in the Administrative Appeals Tribunal (AAT).

The Minister can initiate proceedings in the Federal Court to seek civil remedies for non-compliance with the security obligation. The Minister may also issue a direction to take remedial action to address non-compliance with a risk or security obligation.

Information gathering power

Section 315C of the Act enables the Secretary of the Department of Home Affairs (or the Director-General of Security, ASIO if authorised), to request information or documents from a C/CSP for the purpose of assessing compliance with the security obligation.

This provision is necessary to ensure that the Government can access the relevant information needed to make an assessment regarding the C/CSP's compliance with its obligations and to assess the risk to security. To ensure the relevant information is accessible, section 315D removes the privilege against self-incrimination; a C/CSP cannot refuse to comply with a direction on the grounds it may incriminate a person or expose the person to a penalty.

The information-gathering power is intended to be used as a last resort and in circumstances where a C/CSP considers it is restrained from sharing information for contractual or other legal reasons, or for some other reason refuses to cooperate.

Transparency and accountability measures

Information requested is limited to material directly relevant to monitoring compliance with the proposed security obligation. This requirement increases the likelihood that information obtained will be commercial and unlikely to interfere with the privacy of telecommunications customers in most cases. If disclosure of personal information is required as part of a request for relevant information by the government it will be subject to the *Privacy Act* and offers statutory protection for breach of confidentiality provisions in contracts.

The Secretary must have regard to the costs for the C/CSP in complying with any requirement in the notice that would be likely to be incurred by the C/CSP. In practice, the CAC will engage the C/CSP prior to issuing a notice to discuss the terms of the notice.

The purpose of this discussion will be to ensure the notice targets the information sought and does not put the C/CSP to unnecessary expense. There may be circumstances where it is not feasible or necessary to engage the C/CSP prior to issuing the notice. A failure to engage or consult does not affect the validity of the notice as it is not a pre-condition for issuing the notice.

Written notice

A formal notice requesting information and or documents must be made by written notice and include:

- timeframe for the provision of information;
- the form in which the C/CSP is required to provide/produce the information or documents; and
- outline the effect of provisions relevant to C/CSPs concerning compliance with the Act and offences under the Criminal Code for providing false or misleading information.

This ensures C/CSPs understand the consequences of failure to comply with a notice issued under section 315C, including the criminal consequences for providing misleading or false information.

A carrier or carriage service provider issued with a notice to produce information or documents must comply with that notice and within the specified timeframe, even if it exposes the person (an individual or a body corporate) to criminal or civil liability.

The Minister can initiate proceedings in the Federal Court to seek civil remedies for non-compliance with the security obligation and a direction – these include penalties, enforceable undertakings and injunctions.

Glossary

This glossary describes key terms used in these guidelines; they are not intended to be a legal definition. The descriptions are also specific to these guidelines only and should not be relied upon in other contexts.

Availability	Availability is about ensuring that authorised users have access to information, communications and telecommunications networks and facilities when required. An example where networks and facilities are not available would be a denial-of-service attack which prevents the ordinary functioning of the service, which could have serious economic, social or other consequences (particularly in an emergency).
Carrier	A carrier is defined in the *Telecommunications Act 1997* to mean the holder of a carrier licence.
Carriage service provider	A carrier service provider (CSP) is defined by the *Telecommunications Act 1997* to be a person who supplies, or proposed to supply, a listed carriage service to the public using: • a network unit owned by one of more carriers, or • a network unit in relation to which a nominated carrier declaration is in force. A CSP also includes an international CSP, a secondary user of an exempt network unit, an intermediary and a specified person declared by the Minister as a CSP.
Carriage service intermediary	A carriage service intermediary (CSI) is defined in the *Telecommunications Act 1997* as a person who is a carriage service provider under subsection 87(5) of that Act. To summarise, carriage service intermediaries are middle persons that act between carriage service providers and customers to arrange supply of a service for reward.
Communications Access Co-ordinator	The Communications Access Co-ordinator (CAC) is a position in the Department of Home Affairs established under section 6R of the *Telecommunications (Interception and Access) Act 1979.*
Confidentially	Confidentiality relates to the obligations under 313 (1A) and (2A) of the *Telecommunications Act 1997* to protect information and communication from unauthorised access or unauthorised interference for the purpose of security.
Nominated carriage service provider	A carriage service provider covered by a declaration in force under subsection 197(4) of the *Telecommunications (Interception and Access) Act 1979.*
Telecommunications service	Telecommunications service is defined in the *Telecommunications (Interception and Access) Act 1979* as a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radio communication.
Telecommunications system	Telecommunications system is defined in the *Telecommunications (Interception and Access) Act 1979* as (a) a telecommunications network that is within Australia; or (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia.

Appendix A – Information sharing partners

ASIO Business Government Liaison Unit (BGLU)

The BGLU (https://www.bglu.asio.gov.au/) can be contacted for further threat advice. ASIO's BGLU provides a public interface between the Australian Intelligence Community and Australian business. The BGLU administers a secure website on a free subscription basis. The website contains intelligence-derived unclassified ASIO reporting on the domestic and international security environment as well as physical, personnel and information security advice. The website also contains reports from other Australian Government agencies and international partners.

Australian Signals Directorate (ASD)

The Australian Signals Directorate (ASD) is a vital member of Australia's national security community, working across the full spectrum of operations required of contemporary signals intelligence and security agencies: intelligence, cyber security and offensive operations in support of the Australian Government and Australian Defence Forces (ADF). ASD defends Australia from global threats and advances our national interests through the provision of foreign signals intelligence, cyber security and offensive cyber operations.

Key cyber security information structures within ASD are the Australian Cyber Security Centre (ACSC) and the Computer Emergency Response Team (CERT Australia).

Australian Cyber Security Centre (ACSC)

The ACSC provides advice to Australian organisations, and collects and reports on the threats that networks face from cyber espionage, cyber-attacks and cybercrime. Key ACSC delivered information security programs and advice includes:

- Strategies to Mitigate Cyber Security Incidents
- Australian Government Information Security Manual
- Evaluated Products List
- Cloud Computing Security
- Information security

Office of the Australian Information Commissioner (OAIC)

A robust data breach response plan is important should any data breaches occur (whether or not involving personal information). Further information on responding to data breaches is available in the OAIC resource *Data breach notification — A guide to handling personal information security breaches*[14].

C/CSPs are strongly encouraged to report to OAIC any incidents or breaches involving personal information where there is a real risk of serious harm to individuals. The OAIC can provide general information about obligations under the Privacy Act, factors to consider in responding to a data breach, and steps to take to prevent similar future incidents. The OAIC's *Data breach notification — A guide to handling personal information security breaches* contains information about notifying and responding to an incident or breach. To report a breach email enquiries@oaic.gov.au

[14] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

TISN Communications Sector Group (CSG)

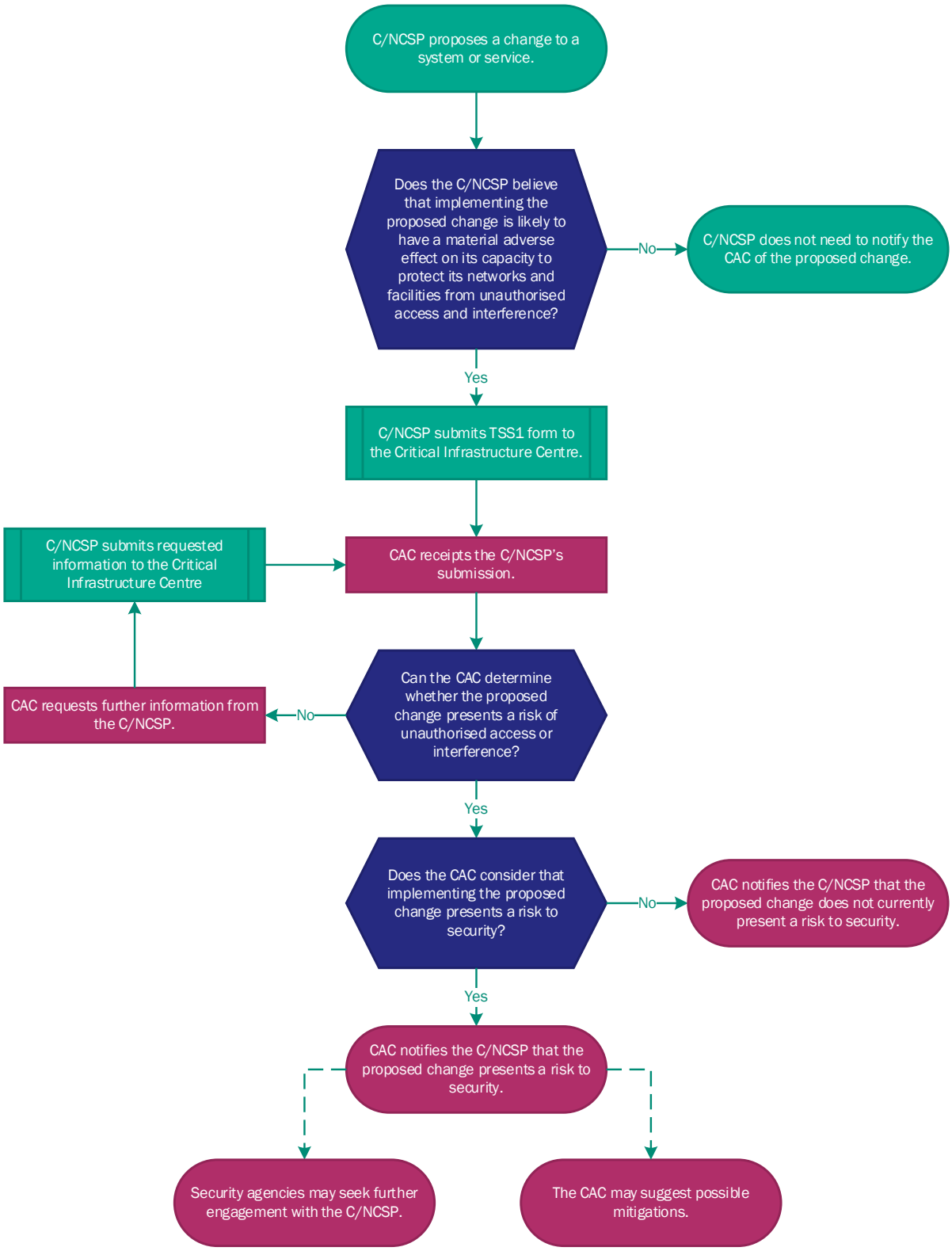
The Trusted Information Sharing Network (TISN) (www.tisn.gov.au) Communications Sector Group (CSG) is one of the key mechanisms for Government to provide security advice to telecommunications providers. The Centre and security agencies will use this forum to provide updates about national security risks to the communications sector, share information and techniques required to assess and mitigate risks, and build capacity within organisations so they are better able to respond to risks and develop a common approach to organisational resilience.

To join the CSG interested parties must demonstrate they are owners and operators of communications critical infrastructure, and provide a company biography to the CSG Secretariat.

Once the CSG Secretariat has received a company biography and verified that the applicant owns or operates communications critical infrastructure, a formal vote is put to the corporate/non-government members of the CSG. This can be done out-of-session, with a majority vote (of those that voted) making the final decision. New members are required to sign a TISN confidentiality deed.

The Department of Communications and the Arts provides Secretariat support to the CSG. They can be contacted at csg@communications.gov.au.

Appendix B – Notification process chart



Appendix C – Resources to help you meet your national security obligation

The following resources may assist with compliance with the security obligation.

- *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines* deals with risk generally.
- *ISO 27001:2013 Information security management* helps organisations keep information assets secure.
- The International Telecommunications Union *Recommendation X.1051 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 2700215* provides guidance on information security management in telecommunications organisations.
- The Australian Signals Directorate:
  - *Information Security Manual*[16] is the standard for the security of government ICT systems
  - *Cloud Computing Security*[17] can help businesses perform a risk assessment and use cloud services securely
- *Strategies to Mitigate Targeted Cyber Intrusions*[18] provides information about how organisations can select the best mitigation strategies for their requirements.
- The *Protective Security Policy Framework* outlines a range of information to effectively managing protective security risk, including controls. Information can be found at www.protectivesecurity.gov.au.
- The Australian Communications and Media Authority publishes information about legal obligations on C/CSPs. This information can be accessed at www.acma.gov.au under 'law enforcement'.

The United Kingdom Cyber Essentials Scheme: Requirements for basic technical protection from cyber-attacks[19] is an accessible guide for organisations of all sizes to mitigating the most common internet based threats to cyber security.

The United Kingdom National Cyber Security Centre, *Cloud Security Collection* is a comprehensive suite of documents to assist organisations in how to configure, deploy and use cloud services securely.[20]

The United States National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[21] includes standards, guidelines, and practices to help owners and operators of critical infrastructure to manage cybersecurity-related risk. It can help organisations determine their current cybersecurity capabilities, set goals for a target level of cyber resilience and establish a plan to improve and maintain cybersecurity.

Further assistance can be obtained from other non-government sources such as:

- MITRE Common Vulnerabilities and Exposures (CVE)
- MITRE Adversarial Tactics, Technologies & Common Knowledge (ATT&CK)
- NIST Computer Security Resource Centre (CSRC)

[15] Available at www.itu.int/rec/T-REC-X.1051

[16] Available at www.asd.gov.au/infosec/ism/

[17] Available at http://www.asd.gov.au/infosec/cloudsecurity.htm

[18] Available at www.asd.gov.au/infosec/mitigationstrategies.htm

[19] Further information is available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

[20] Available at www.ncsc.gov.uk/guidance/cloud-security-collection

[21] Further information is available at www.nist.gov/cyberframework/