Cyber incident notification regulations in Australia

PwC's quick guide to cyber incident regulatory notification obligations for organisations in Australia

September 2023

www.pwc.com.au

pwc

1
Introduction

No industry remains untouched by the technology and data revolution.

As organisations have continued to venture further into the digital realm, the risk profile of their organisation and operations has evolved significantly. The great opportunities that come with increased digitisation also brings the risk that threat actors or significant cyber events can disrupt and damage business and their stakeholders. With this change, we have seen a significant shift in focus from regulators and law enforcement, with their eyes fixed on the cybercrime scourge.

From the Office of the Australian Information Commission (**OAIC**) to the Australian Prudential Regulation Authority (**APRA**), regulators are lining up to ensure that the organisations that they are tasked with regulating are appropriately prepared for the 21st century digital threat environment.

A key area where we are seeing significant overlap across regulators and jurisdictions is notification obligations where a cyber incident has occurred that has impacted the organisation.

1.2
Cyber incident and data breach notification

After any major cyber incident, organisations need to, among many other concerns, consider their exposure, obligations and strategy in relation to management of their cyber incident response in a timely manner. There is no doubt that communication with key stakeholders is a critical part of managing an organisation's risk and exposure from a cyber incident. In doing so, it is essential for an organisation to understand who it is legally required to notify, who it should notify, and who it wants to notify voluntarily.

There are a range of stakeholders that organisations need to consider when it comes to notification of cyber incidents – **the diagram below** sets out some of the key stakeholders that organisations may consider in developing their communications and notification strategy.

- Regulatory bodies
- Law Enforcement
- Market Operators
- Customers & Suppliers
- Employees
- Insurers
- Joint venture/alliance partners
- The public/individuals

A key question that arises in these circumstances is whether an organisation is legally required to notify a particular stakeholder of the cyber incident.

Legal obligations to notify can come from a range of instruments. **The diagram below** sets out some examples of where organisations may have a legal obligation to notify a particular stakeholder of a cyber incident.

Regulatory body

Obligation may arise from the governing legislative instrument or regulations/rules/licences issued by a regulator

Law enforcement

Obligation may arise from the legislative requirements to report certain events

Market operators

Obligation may arise from the applicable market listing rules

Customers & suppliers

Obligation may arise from the contract between the organisation and the supplier/customer

Employees

Obligation may arise from collective bargaining/enterprise bargaining arrangements

Insurers

Obligation may arise from the insurance contract in place with the insurer

Joint venture/alliance partners

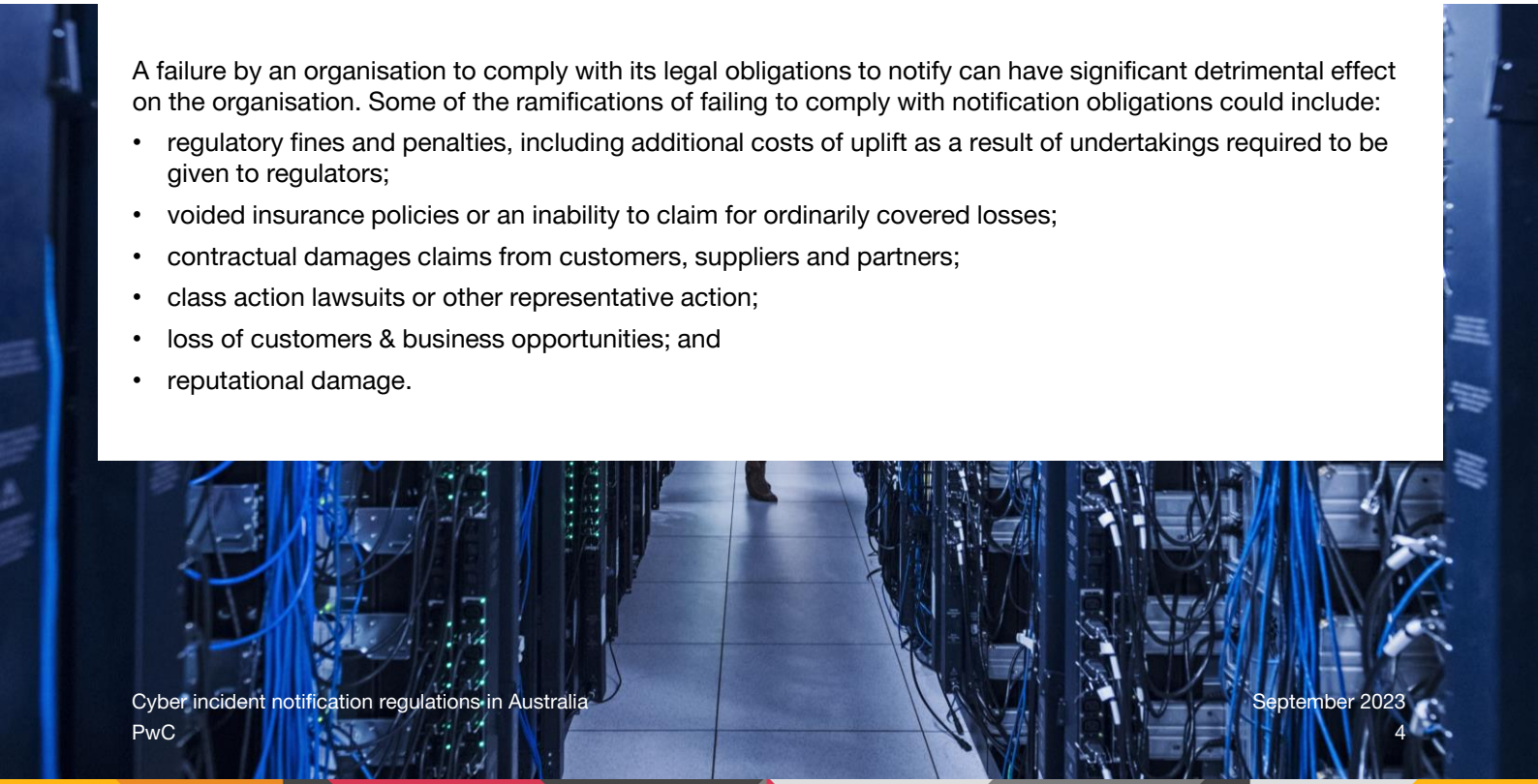
Obligation may arise from the relevant JV/partnering arrangements

Wider public/individuals

Obligation may arise from laws requiring notification of impacted individuals

A failure by an organisation to comply with its legal obligations to notify can have significant detrimental effect on the organisation. Some of the ramifications of failing to comply with notification obligations could include:

- regulatory fines and penalties, including additional costs of uplift as a result of undertakings required to be given to regulators;
- voided insurance policies or an inability to claim for ordinarily covered losses;
- contractual damages claims from customers, suppliers and partners;
- class action lawsuits or other representative action;
- loss of customers & business opportunities; and
- reputational damage.



1.3
What this guide is for

As mentioned earlier, it is important that an organisation gets compliance with its notification obligations right.

This Guide concentrates on the **first set of legal obligations** that an organisation may have to notify a stakeholder of a cyber incident, namely notifications to regulatory bodies. The Australian legal landscape in the cyber incident space is somewhat complex, with federal economy-wide obligations to notify of a cyber incident in certain circumstances, supplemented with industry-specific and state-based laws, which may apply depending on the nature of the organisation.

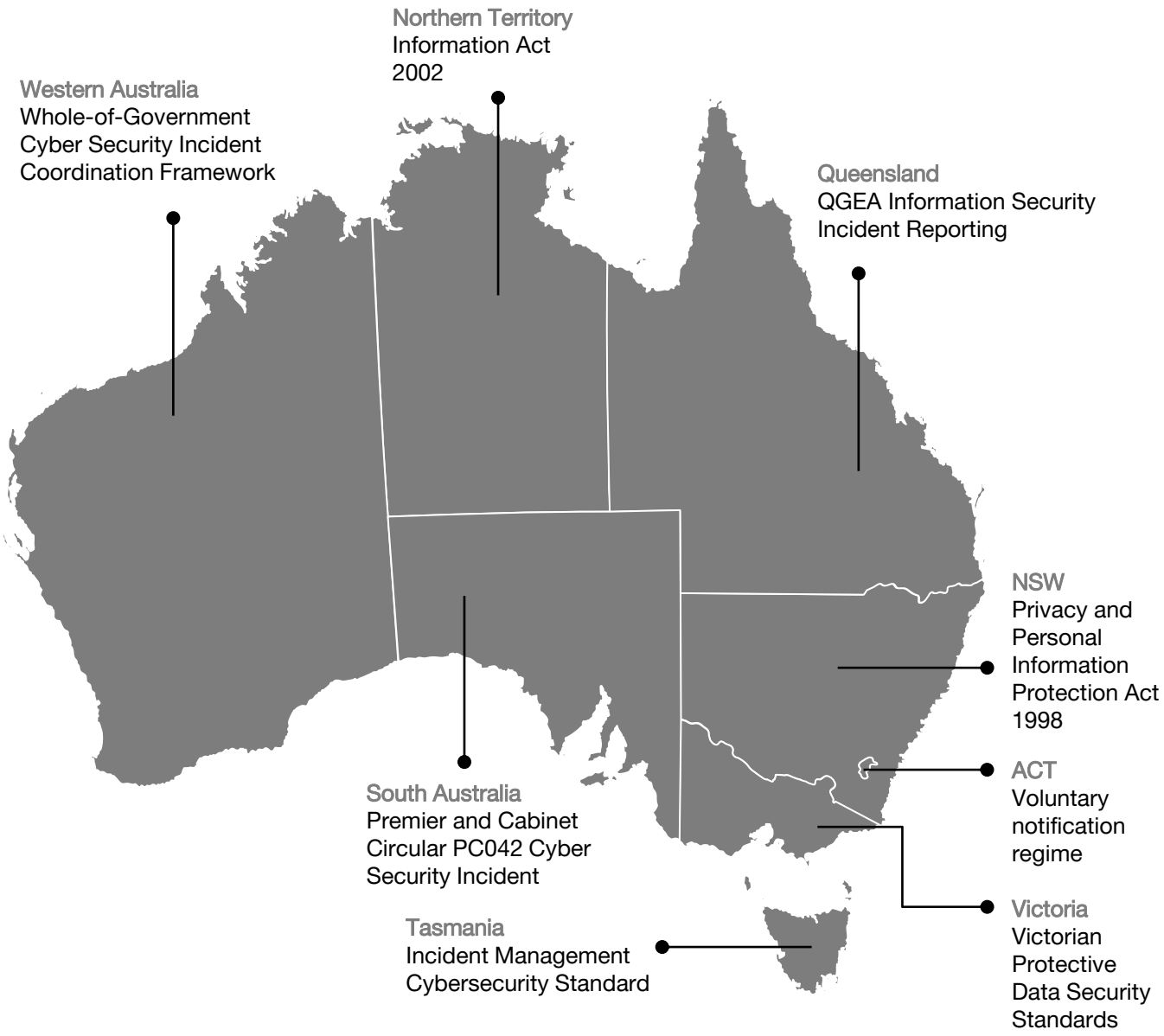
Set out in this guide is a list of the key cyber incident notification obligations that currently apply in the Australian legal landscape. For each of the regulatory obligations, we have summarised the following information:

Information in the guide

- The jurisdiction for the notification obligation
- The source of the notification obligation
- Who the notification obligation applies to
- Who the regulator is
- The trigger for the notification obligation
- Who needs to be notified
- The required timing of the notification
- The information that needs to be contained in the notification
- The notification form requirements
- Some key issues to consider in complying with the notification requirement

Please note that this is not legal advice. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

1.4
In this guide...



All of Australia (sectoral legislation)

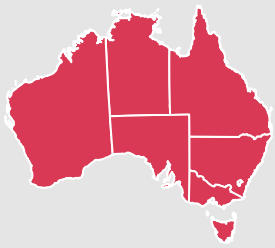
- Privacy Act
- Security of Critical Infrastructure
- Telecommunications
- Prudential Standards (CPS 234, 232, 230)
- Consumer Data Right
- ASX Listing Rules
- My Health Records

Contents

Contents

2
Privacy Act 1988 (Cth) – Notification of eligible data breach

Summary: An APP Entity must notify the OAIC and affected individuals when a data breach involving personal information is likely to result in serious harm



Source?
Part IIIC of the Privacy Act 1988 (Cth)

Regulator?
Office of the Australian Information Commissioner (**OAIC**)

Who to notify?

- OAIC
- Affected individuals (being those individuals whose personal information was affected by the data breach)

Who needs to notify?

- APP Entities
- Australian Government (and Norfolk Island Government) agencies, but does not include State and Territory agencies
- Organisations (which includes an individual, body corporate, partnership, unincorporated association, or trust) but excludes:
- small business operators (<$3m annual turnover)*
- registered political party;
- State or Territory authority; or a prescribed instrumentality of a State

When to notify?

- As soon as practicable after becoming aware of an eligible data breach.
- Where a data breach is only suspected, the APP Entity has 30 days to investigate.

Trigger for notification

An entity must notify the OAIC and affected individuals if:

a) it has reasonable grounds to believe that an eligible data breach has occurred; or
b) it is directed to do so by the OAIC.

An eligible data breach happens if:

a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not.

Notice contents

The notification to the OAIC and the affected individuals must contain:

- The APP entity's details;
- A description of the eligible data breach;
- The kinds of information concerned; and
- Recommended steps individuals should take in response to the breach.

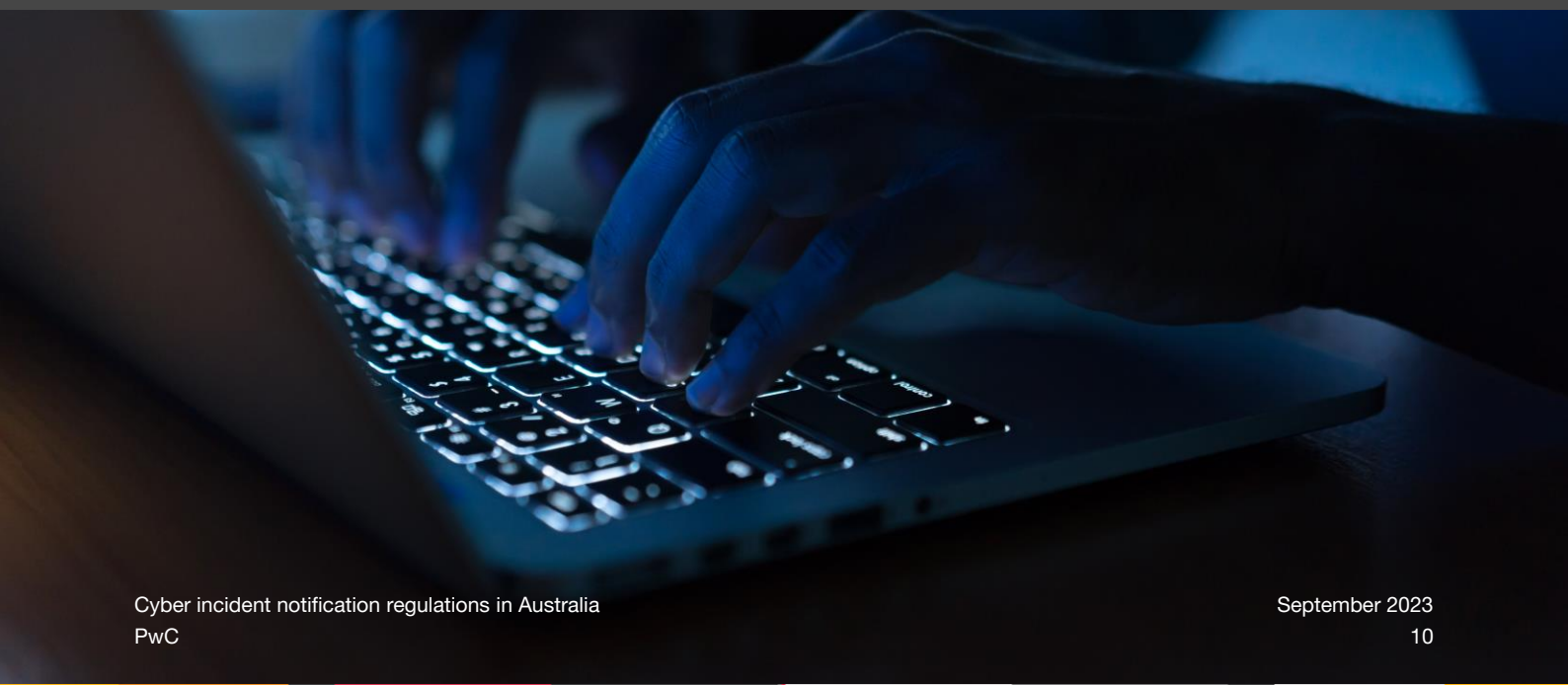
Notice form

Eligible data breaches are reported to the OAIC through the online notification portal.

APP Entity to notify individual as it would ordinarily communicate them. Where it is not possible to contact the relevant individuals, the APP Entity may have to make a public statement available on its website.

Key considerations

- The NDB test is two limbs – the first limb is whether reasonable grounds to believe that an eligible data breach has occurred, and the second limb is whether that breach is likely to cause 'serious harm'. Both need to be established for notification to be required.
- Not only does there need to be 'serious harm', it needs to be *more likely than not* that the 'serious harm' will occur as a result of the relevant data breach.
- Assessment of the likelihood of 'serious harm' can be difficult to conduct as it will depend on the circumstances surrounding the data breach, such as the nature of the information breached, the threat actor, and whether the data has been leaked.
- One of the biggest challenges of applying the NDB test is situations where organisations are aware unauthorised access/disclosure has occurred but lack the evidence/ability to conclude whether information has actually been exfiltrated. The OAIC has stated that merely communicating that there has been no evidence of exfiltration is likely to be insufficient. Organisations must be careful with their messaging and level of investigation they conduct in assessing whether an eligible data breach has occurred.
- Organisations should consider whether an exemption to notification may apply (e.g. employee records data). Organisations may apply to the OAIC to exempt certain breaches from notification, however these exemptions are rarely granted.
- At times, one single data breach will affect multiple organisations. In such cases, the OAIC has recommended that only the entity with the 'most direct relationship' to the impacted individuals should make the notification.
- Australian organisations must consider the extraterritorial application of other jurisdictional privacy regulations that contain cyber incident notification obligations e.g. the EU General Data Protection Regulation (**GDPR**).
- The Australian Government in early 2023 released its long-awaited review report of the Privacy Act. The report proposes a new 72-hour window (similar to the GDPR) for APP entities to report eligible data breaches to the OAIC – this is a significant restriction from the current obligation to report "as soon as reasonably practicable". It is likely this proposal will be enshrined in law given the desire to align the Australian federal Act to the GDPR.



3
Security of Critical Infrastructure Act 2018 (Cth) – Notification of cyber security incidents

Summary: 'Responsible entities' for critical infrastructure assets must report and notify the ACSC when certain cyber security incidents occur.

Source?
Sections 30BC and 30BD of the Security of Critical Infrastructure Act 2018 (Cth)

Regulator?
Australian Cyber Security Centre (**ACSC**)

Who to notify?

- The relevant Commonwealth body as stipulated under the Act in section 30BF. This is currently the ACSC.

Who needs to notify?

- 'Responsible entities' must notify. They are the entities that are most closely linked to a critical infrastructure asset (CI asset).

The responsible entity is defined separately for each asset class e.g. the responsible entity in respect of a critical water asset is the utility that holds the licence to operate that asset under applicable State laws.

When to notify?

- **'Critical' cyber security incident** – within 12 hours of becoming aware.
- **'Other' cyber security incident** – within 72 hours of becoming aware

Trigger for notification

An entity must notify the ACSC if a 'critical cyber security incident' or an 'other cyber security incident' has occurred.

- **Critical cyber security incidents** are those which have occurred or are in progress, where the incident has had, or is having, a 'significant impact' on the availability of the CI asset.

A significant impact is one where there has been material disruption of the availability of the essential goods or services delivered by a CI asset.

- **Other cyber security incidents** with a relevant impact which have occurred, are in progress or are imminent.

A relevant impact is one where it has, is, or is likely to impact the CI asset's availability, integrity or reliability, or impact the confidentiality of information about the CI asset that is stored in the asset.

Notice contents

Entities will be asked to provide the following in a report:

- contact information;
- organisation information (including ABN);
- critical infrastructure sector;
- date and time the incident was identified and whether it is ongoing;
- confirmation whether the incident is having a significant impact on the asset;
- details on the incident, including how it was discovered; its nature (e.g. ransomware), whether the incident affects IT, operational technology, or customer data);
- whether the incident has been reported elsewhere; and
- any other relevant information.

Notice form

Cyber security incidents can be reported either orally to 1300CYBER1, or in writing via an online webform on the ACSC's website at https://www.cyber.gov.au/acsc/report/report-a-cyber-security-incident#no-back

Note that any oral report must be followed by a written record within

a) 84 hours of verbal notification for critical incidents; and

b) b) 48 hours for other incidents.

Key considerations

- The SOCI framework is complex and nuanced. In the first instance, entities must undertake a careful legal and factual analysis in order to define the scope of its assets and whether it falls within the realm of a CI asset. Failure to do so may result in a compliance gap.
- Organisations will need to consider what materiality they will apply to particular assets around the impact of cyber incidents to ensure quick and appropriate classification of incidents as either a 'critical' cyber security incident or an 'other' cyber security incident.
- The SOCI Act regulates a range of stakeholders in relation to critical assets – even if you do not operate or own an CI asset, you may still have obligations in relation to those assets as an integral part of the supply chain.
- Certain entities may have assets sitting outside its core operations that may also be considered CI assets. Entities must be aware that its services and assets can be captured under multiple sectors, and must assess each of these against the specific asset definitions set out in the SOCI Act.
- Compliance with SOCI also requires broad consideration of third party risk management including physical, supply chain etc., which requires enterprise level coordination. Mapping your current and future state SOCI compliance will require an enterprise lens to ensure that legal and technical measures completely reflect all SOCI obligations.

4
Telecommunications – Cyber security incident notification

Summary: Carriers and certain carriage service providers must inform the ASD of cyber security incidents that have had or are having a significant or relevant impact on a telecommunication asset.

Source?
Telecommunications Act 1997 (Cth)
Telecommunications (Carrier License Conditions – Security Information) Declaration 2022
Telecommunications (Carriage Service Provider – Security Information) Determination 2022
Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)

Regulator?
- Australian Communications and Media Authority (**ACMA**)
- Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Who to notify?

- ACSC of the Australian Signals Directorate (**ASD**)
- Where information pertains to CI assets, notify the CISC.

Who needs to notify?

- All carrier licence holders and eligible carriage service providers (**CSP**).
- Carrier licence holder has the meaning given by the *Telecommunications Act* 1997 (Cth).
- Eligible carriage service providers has the meaning given by the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).

When to notify?

- **Cybersecurity incidents that have 'significant impact'** – as soon as practicable and within at least 12 hours of the carrier/eligible CSP becoming aware of the incident
- **Cybersecurity incidents that have 'relevant impact'** – as soon as practicable and within at least 72 hours of the carrier/eligible CSP becoming aware of the incident

Trigger for notification

An entity must notify the ACSC if a 'critical cyber security incident' or an 'other cyber security incident' has occurred.

- **Critical cyber security incidents** are those which have occurred or are in progress, where the incident has had, or is having, a 'significant impact' on the availability of the CI asset.

A significant impact is one where there has been material disruption of the availability of the essential goods or services delivered by a CI asset.

- **Other cyber security incidents** with a relevant impact which have occurred, are in progress or are imminent.

A relevant impact is one where it has, is, or is likely to impact the CI asset's availability, integrity or reliability, or impact the confidentiality of information about the CI asset that is stored in the asset.

Notice contents

The ACSC webform asks for the following information:

- contact information;
- organisation information (including ABN);
- critical infrastructure sector;
- date and time the incident was identified and whether it is ongoing;
- confirmation whether the incident is having a significant impact on the asset;
- details on the incident, including how it was discovered; its nature (e.g. ransomware), whether the incident affects IT, operational technology, or customer data);
- whether the incident has been reported elsewhere; and
- any other relevant information.

Notice form

Cyber security incidents can be reported either orally to the ASD or in writing via an online webform on the ACSC's website at https://www.cyber.gov.au/acsc/report/report-a-cyber-security-incident#no-back

Key considerations

- The reporting obligations apply to any cybersecurity incident involving assets belonging to a carrier or eligible CSP. The broad definition of 'assets' means that a large range of tangible assets used to supply a carriage service is captured. This can include telecommunication networks, computers, computer programs or computer data.
- The mandatory notification obligation applies individually to each carrier in a corporate group. However, another carrier in the group can provide cyber incident notifications on behalf of other carrier licensees.
- ACMA also plays an important role from a cybersecurity perspective, and may launch investigations in relation to cyber incidents in the telecommunications sector. In particular, these will be focussed on compliance with telecommunications legislation.
- Some overlap exists between the SOCI rules, which govern critical telecommunication assets and related sector assets, and the existing telecommunications regulation. Care must be taken to navigate the conflicting telecommunication and the SOCI rules.

5
CPS 234 (Information security) – Notification of information security incident

Summary: If an APRA-regulated entity becomes aware that it has breached an information security incident or it is aware of a material information security control weakness, it must notify APRA accordingly.

Source?
CPS 234 (Information Security)

Regulator?
- APRA

Who to notify?

- APRA

Who needs to notify?

All APRA-regulated entities, defined in CPS 234 as:

- authorised deposit-taking institutions **(ADIs)**, including foreign ADIs, and non-operating holding companies authorised under the Banking Act (authorised banking NOHCs);
- general insurers, including Category C insurers, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and parent entities of Level 2 insurance groups;
- life companies, including friendly societies, eligible foreign life insurance companies **(EFLICs)** and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);
- private health insurers registered under the PHIPS Act; and
- RSE licensees under the SIS Act in respect of their business operations.

When to notify?

- **An information security incident:** As soon as possible, no later than 72 hours after becoming aware of an incident
- **A material information security weakness:** As soon as possible, no later than 10 business days after the entity expects it will not be able to remediate the weakness in a timely manner"

Trigger for notification

An APRA regulated entity must notify APRA of an information security incident where the incident has:

a) the potential to materially affect, financially or non-financially, the entity or interests of depositors, policyholders, beneficiaries or other customers; or

b) has been notified to other regulators, either in Australia or other jurisdictions (including domestic government agencies and international regulators).

An **information security incident** occurs if there has been an actual or potential compromise of information security. **Information security** means the preservation of an information asset's confidentiality, integrity and availability.

An APRA regulated entity must also notify a **material information security control weakness** which the entity expects it will not be able to remediate in a timely manner. Information security control means a prevention, detection or response measure to reduce the likelihood or impact of an information security incident.

Notice contents

For an *incident*, the notification must include:

- Entity & APRA contact information;
- Date & time of incident;
- Other agencies notified;
- Description of the trigger event;
- Incident status, severity, type and description;
- Period impacted by the incident; and
- Mitigations taken or planned.

For a *weakness,* the notification must include:

- Entity & APRA contact information;
- Date & time of discovering weakness;
- Impact and description of the weakness; and
- Mitigations taken or planned.

Notice form

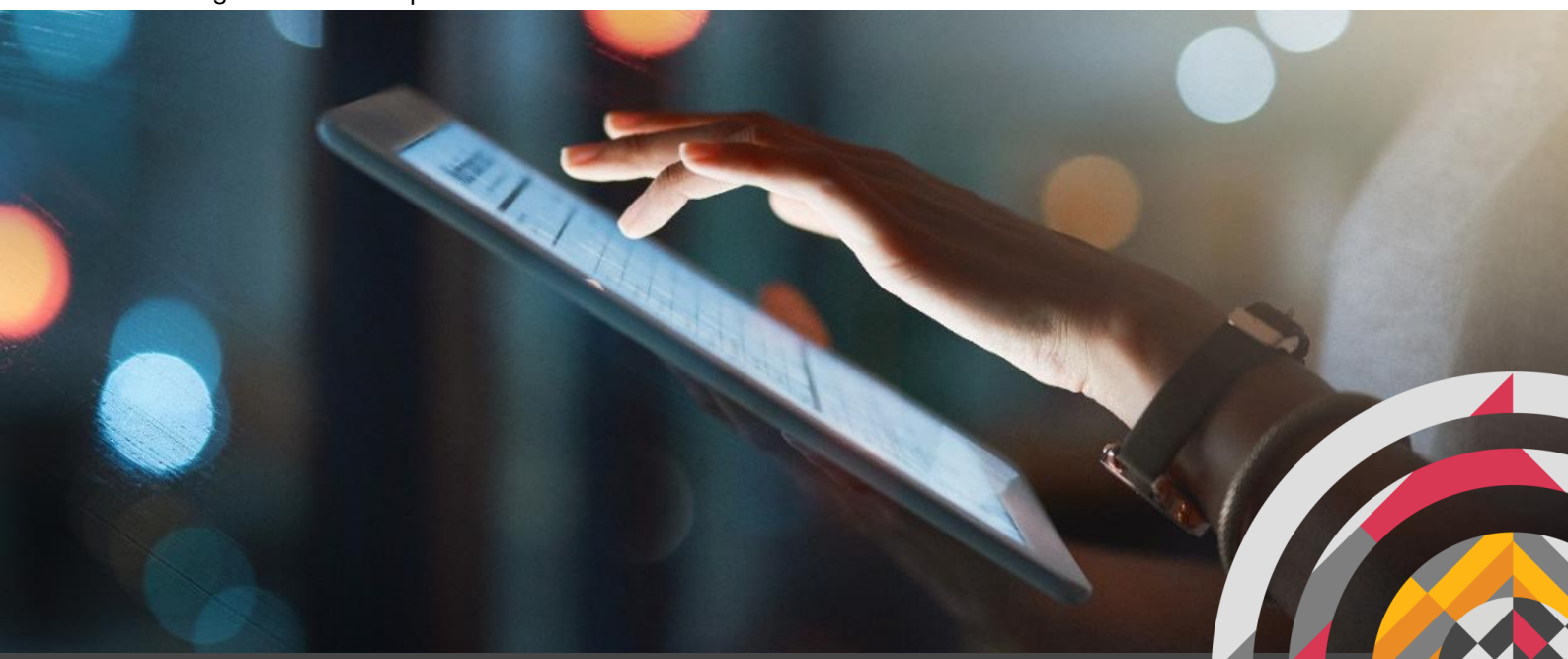
Under CPG234 the following forms are to be used for notifications under CPS234:

Information security incident under paragraph 35 of CPS 234 -

https://apra.au1.qualtrics.com/jfe/form/SV_5cL51HPImtGWr8V

Material information security control weakness notification under paragraph 36 of CPS 234 -

https://apra.au1.qualtrics.com/jfe/form/SV_5mYAnSiYR8tovNr



Key considerations

- The requirement of the notification under this Prudential Standard applies to notifications of information security incidents that are not already captured as notifications under Prudential Standard CPS 231 Outsourcing and Prudential Standard CPS 232 Business Continuity Management (see next page).
- If a cyber incident results in the termination of a material outsourcing arrangement, then APRA-regulated entities must notify APRA in accordance with CPS 231.
- With the final release of APRA's new Prudential Standard CPS 230 Operational Risk Management (see page 19 of this guide), APRA has also confirmed that a notification of an information security incident under this CPS 234 does not need to be separately reported under CPS 230.

6
CPS 232 (Business continuity management) – Notification of major disruption

Summary: An APRA-regulated institution must notify APRA after the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness.

Source?
CPS 232 (Business Continuity Management)

Regulator?
- APRA

Who to notify?

- APRA

Who needs to notify?

All APRA-regulated entities, defined in CPS 232 as:

- authorised deposit-taking institutions **(ADIs),** including foreign ADIs, and non-operating holding companies authorised under the Banking Act (authorised banking NOHCs);
- general insurers, including Category C insurers, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and parent entities of Level 2 insurance groups; and
- life companies, including friendly societies, eligible foreign life insurance companies **(EFLICs)** and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs).

When to notify?

- As soon as possible and no later than 24 hours.
- The APRA-regulated institution must notify APRA when normal operations resume.

Trigger for notification

An APRA regulated institution must notify APRA of an incident if the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness

Notice contents

There is currently no form published on the APRA website for this standard however the standard requires the organisation to provide details of:

- the nature of the disruption;
- the action being taken;
- the likely effect; and
- the timeframe for returning to normal operations.

The organisation must also must notify APRA when normal operations resume.

Notice form

The Prudential Standard outlines that notifications must be given in such a form, if any, as APRA determines and publishes on its website from time to time.

There is currently no form published on the APRA website for this standard.

Key considerations

- This Prudential Standard is most likely to apply where a cyber attack significantly impacts a regulated entities ability to function, for example: a major ransomware attack encrypting the key parts/entirety of the entity's information technology systems.
- This Prudential Standard applies whether or not activities are outsourced to related bodies corporate or third-party service providers.
- This Prudential Standard also applies to arrangements where the service provider is located outside Australia or the functions are performed outside Australia.
- If a cyber incident results in the termination of a material outsourcing arrangement, then APRA-regulated entities must notify APRA in accordance with CPS 231.
- The recently finalised CPS 230 will replace this CPS 232 when it comes into effect on 1 July 2025. As a result, whilst organisations should ensure compliance with CPS 232 now, it will be prudent to look to any uplift required to align with the requirements of CPS 230 (outlined on page 19 of this guide).

7

CPS 230 (Operational risk management) – Notification of operational risk incidents

Summary: CPS 230 replaces CPS 231 and CPS 232, and will operate alongside CPS 220, CPS 234 and APS 222. The proposed effective date is 1 July 2025 for most entities. Under this Standard, an APRA-regulated institution must notify APRA after the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness.

Source?
CPS 230 (Operational Risk Management)

Regulator?
- APRA

Who to notify?

- APRA

Who needs to notify?

All APRA-regulated entities, defined in CPS 230 as:

- authorised deposit-taking institutions **(ADIs)**, including foreign ADIs, and non-operating holding companies authorised under the Banking Act (authorised banking NOHCs);
- general insurers, including Category C insurers, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and parent entities of Level 2 insurance groups;
- life companies, including friendly societies, eligible foreign life insurance companies **(EFLICs)** and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);
- private health insurers registered under the PHIPS Act; and
- RSE licensees under the SIS Act in respect of their business operations.

When to notify?

- As soon as possible and no later than 72 hours for a operational risk incident **OR** 24 hours where it has suffered a disruption to critical operations outside of tolerance.

Trigger for notification

An APRA-regulated entity must notify APRA after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations **OR** if it has suffered a disruption to a critical operation outside tolerance.

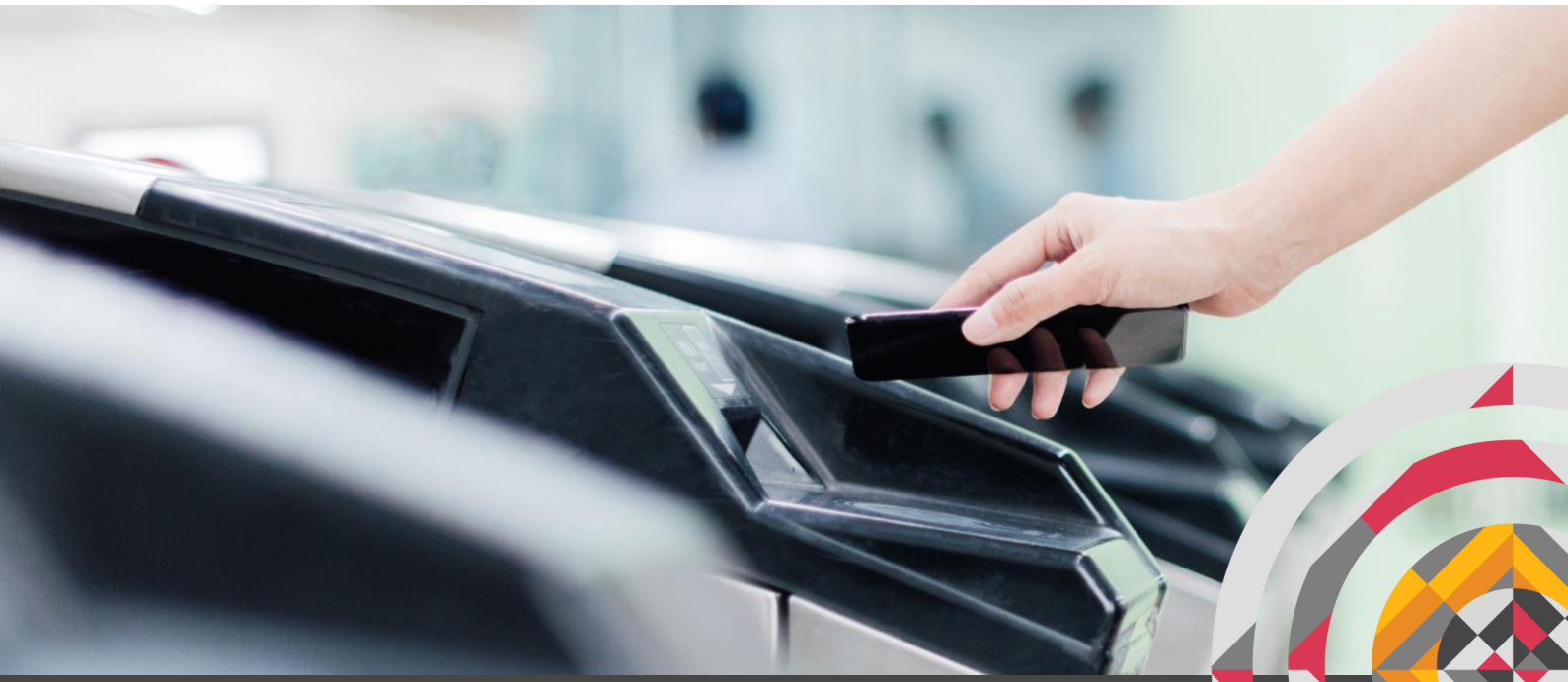
Notice contents

The contents of the notice has not yet been prescribed by APRA. Where the organisation has suffered a disruption to a critical operation outside tolerance, the standard requires that the organisation provide details of:

- the nature of the disruption;
- the action taken;
- the likely impact on the entity's business operations; and
- the timeframe for returning to normal operations.

Notice form

The notice form has not yet been prescribed by APRA.



Key considerations

- Draft Prudential Practice Guide CPG 230 has been released to accompany the final CPS 230. Consultation will take place on CPG 230 until 13 October 2023. The guidance does not clarify what "material financial impact" and "material impact" means.
- Whilst CPS230 officially commences on 1 July 2025, for existing service provider arrangements, APRA-regulated entities will have until the earlier of 1 July 2026 or the next renewal date of an existing agreement to ensure compliance with CPS 230. Whilst there is a transitional period allowed, it is imperative that all APRA-regulated entities review their operational risk management processes and arrangements against the Prudential Standard to scope the extent of changes required.
- This new Prudential Standard sits alongside other regulatory requirements and guidance relating to operational risk, including CPS 234 (Information Security) and CPS 226 (Margining and Risk Mitigation for Non-centrally Cleared Derivatives), as well as other APRA cross-industry and industry-specific prudential guides.
- A notification of an information security incident reported under CPS 234 does not need to be separately reported under the notification requirements of this Prudential Standard when it comes into effect.

8

Consumer data right –Notification of eligible data breach

Summary: Under the Consumer Data Right **(CDR)** framework, accredited data recipients and designated gateways must also comply with the Privacy Act's Notifiable Data Breach **(NDB)** scheme in relation to any eligible data breaches involving CDR data (where that data relates to a CDR consumer).

Certain parties participating in the CDR system must also create and maintain plans to respond to security incidents. These plans must include procedures for notifying information security incidents to the Australian Cyber Security Centre **(ACSC).**

Source?
Part IVD of the Competition and Consumer Act 2010
Competition and Consumer (Consumer Data Right) Rules 2020
Part IIIC of the Privacy Act 1988 (Cth)

Regulator?
- APRA

Who to notify?

- OAIC
- CDR consumer holding affected CDR data
- ACSC

Who needs to notify?

- Accredited data recipients
- Designated gateways

An accredited data recipient is an entity that has been accredited by the Australian Competition and Consumer Commission **(ACCC)** under the CDR framework to receive and use CDR data for a specific purpose such as offering certain products and services).

A designated gateway is an entity that has been designated by the Treasurer to facilitate the transfer of CDR data between data holders and accredited data recipients.

The ACSC obligations can also apply to some other parties participating in the CDR system under CDR representative and outsourced service provider arrangements.

When to notify?

- **OAIC and individuals:** As soon as practicable after becoming aware of an eligible data breach.
- **ACSC:** As soon as practicable (and no later than 30 days) after the information security incident occurs.

Trigger for notification

In relation to the obligation to apply with the NDB scheme as it applies to the CDR framework, an accredited data recipient/designated gateway must give a notification if:

a) it has reasonable grounds to believe that an 'eligible data breach' has happened; or

b) it is directed to do so by the OAIC.

An **eligible data breach** happens if:

a) there is unauthorised access to, unauthorised disclosure of, or loss of, CDR data held by an accredited data recipient/designated gateway; and

b) the access, disclosure or loss is likely to result in serious harm to any of the CDR consumer for CDR data.

Notice contents

The notification to the OAIC and the affected CDR Consumer must contain:

- the accredited data recipient/designated gateway's details;
- a description of the eligible data breach;
- the kinds of CDR data concerned; and
- recommended steps CDR Consumer should take in response to the breach.

The ACSC webform asks for the following information:

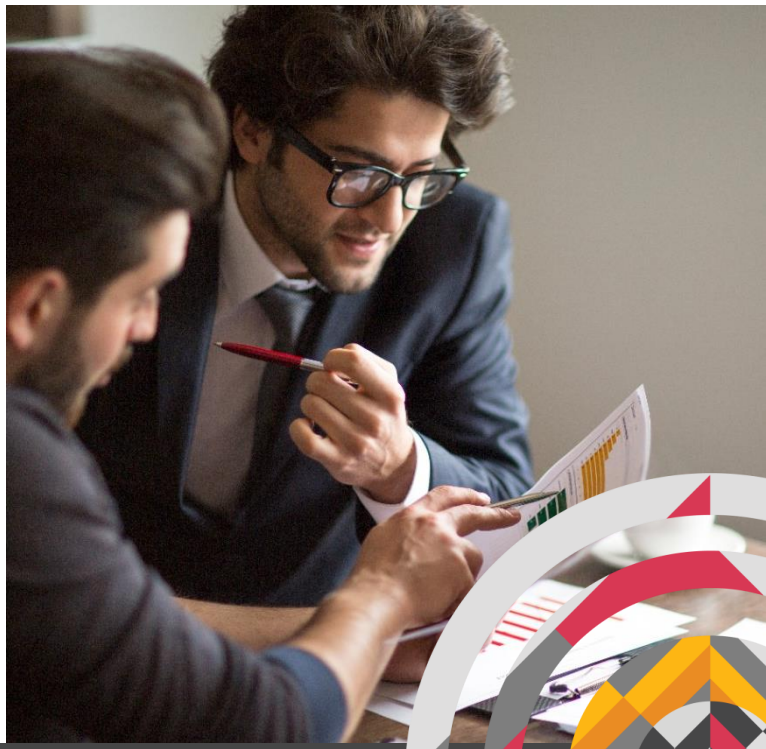
- contact information;
- organisation information (including ABN);
- critical infrastructure sector;
- date and time the incident was identified and whether it is ongoing;
- confirmation whether the incident is having a significant impact on the asset;
- details on the incident, including how it was discovered; its nature (e.g. ransomware), whether the incident affects IT, operational technology, or customer data);
- whether the incident has been reported elsewhere; and
- any other relevant information.

Notice form

Eligible data breaches are reported to the OAIC through the online notification portal at https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion

CDR consumers must be notified via the ordinary means of communication. Where it is not possible to contact the relevant individuals, the accredited data recipient/designated gateway is required to make a public statement available on its website.

Reports to the ACSC are done via an online webform on the ACSC's website at https://www.cyber.gov.au/acsc/report/report-a-cyber-security-incident#no-back



Key considerations

- The OAIC, the ACCC, Data Standards Body, and sector specific regulators are all be involved in regulating the CDR more broadly. As such, it is critical for accredited data recipients/designated gateways to ensure they comply with all obligations required by each regulatory body, noting that there is a separate data breach reporting requirement to both the OAIC and the ACSC.
- Please see our considerations in relation to the NDB Scheme above. Whether accredited data recipients, in practice, would have processes in place to identify which of their information is 'CDR data' versus 'personal information' under the Privacy Act is not clear. It may be the case that some accredited data recipients who suffer a data breach think about their notification obligations because the CDR data that has been breached is 'personal information' for the purposes of the Privacy Act.

9
ASX listing rules – Continuous disclosure obligations

Summary: Entities listed on the ASX are subject to continuous disclosure obligations under the ASX Listing Rules. This means that any information that has a material effect on the price or value of a entities' securities must be disclosed.

As a general rule, data breaches that would reasonably be expected to have a material effect on the price of a listed entity's securities are required to be disclosed to the ASX.

Source?
ASX Listing Rule 3.1
ASX Guidance Note 8

Regulator?
Australian Securities Exchange (ASX)

Who to notify?

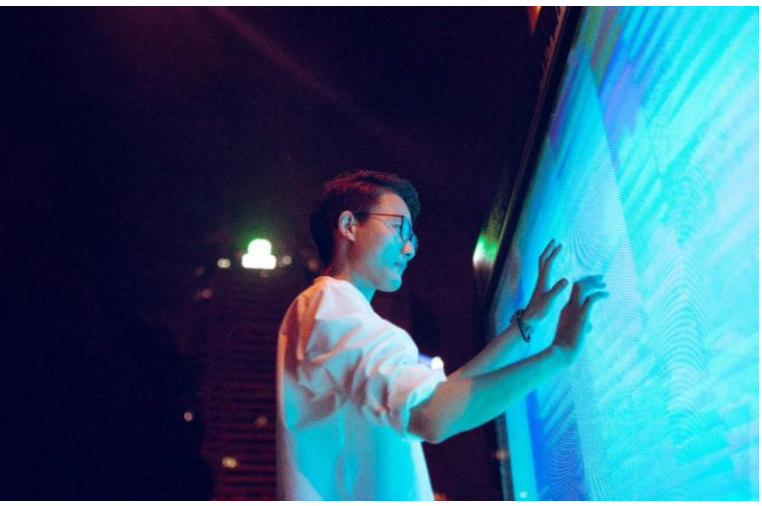
- ASX
- ASX Market Announcements Platform

Who needs to notify?

- ASX-listed entities

When to notify?

- Immediately i.e. as quickly as possible in the circumstances, whilst ensuring there is no unnecessary delay or deferral until a later time.



Trigger for notification

A listed entity must immediately notify the ASX (and subsequently, the ASX will notify the market via the ASX Market Announcements Platform) of any information (e.g. a privacy or security incident) that a reasonable person would expect to have a material effect on the price or value of its securities once it becomes aware of that information.

The continuous disclosure obligation begins once the information that becomes known to the listed entity is 'market sensitive information'.

Market sensitive information is any information that would, or is likely to, influence persons who commonly invest in securities in deciding whether to acquire or dispose of the securities.

Notice contents

Entities must make disclosures to the ASX in the form of a written announcement that is accurate, complete and not misleading.

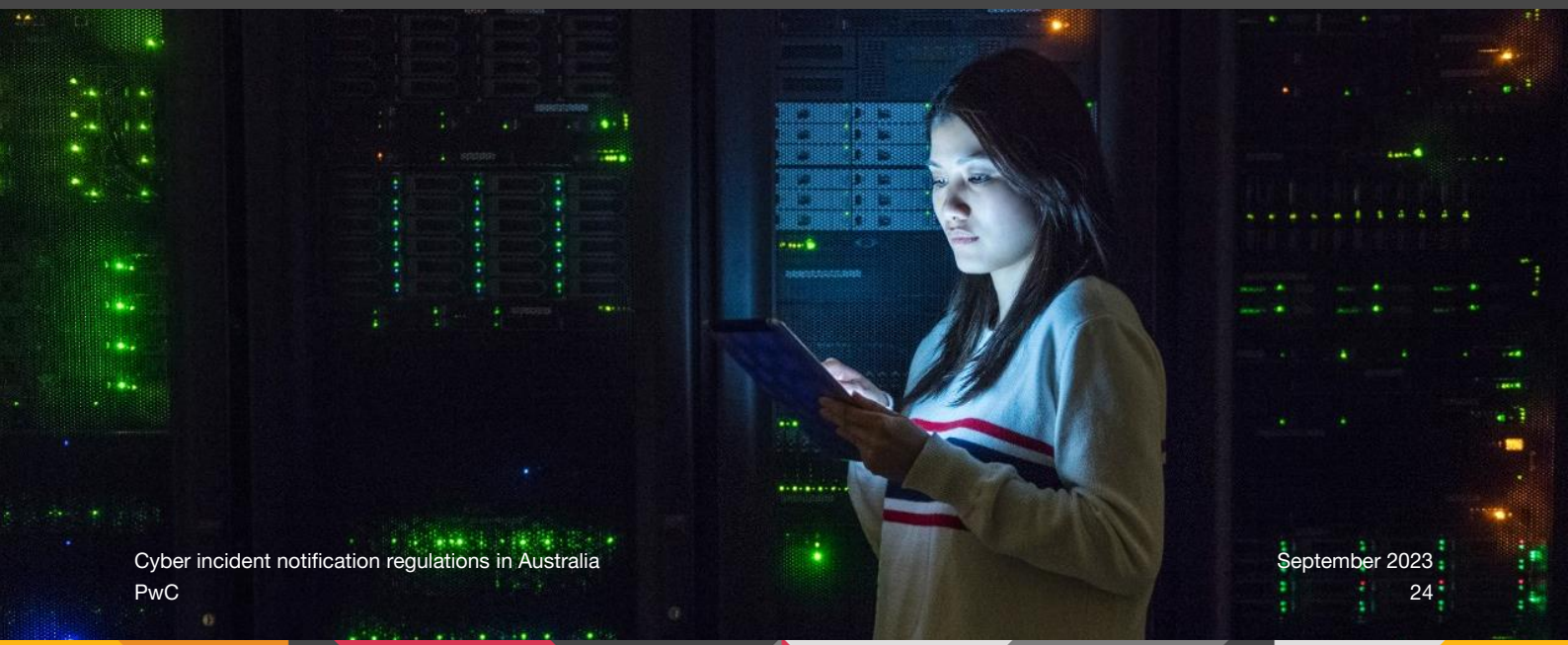
The announcement should contain sufficient detail for investors to assess the impacts of the disclosure on the value of the entity's securities. "Information" extends beyond pure matters of fact and includes matters of opinion and intention.

Notice form

A disclosure must be in the form of a written announcement (as per Listing Rule 19.10) and given to the ASX Market Announcements office for release to the market.

Key considerations

- In the time between the beginning of disclosure obligations and giving an announcement to the ASX for release, the entity should consider whether it is appropriate to request trading halt or voluntary suspension.
- Where the ASX receives disclosures which it considers likely to involve 'market sensitive' information e.g. trade secrets as a result of data breach – it will halt trading in the entity's securities under *ASX Operating rule 3301(a).*
- There are exceptions to the disclosure obligations of the entity concerned IF:
  a) One or more of the following five situations arise:
     i. it would be a breach of a law to disclose the information;
     ii. the information concerns an incomplete proposal or negotiation;
     iii. the information comprises matters of supposition or is insufficiently definite to warrant disclosure;
     iv. the information is generated for the internal management purposes of the entity; or
     v. the information is a trade secret; AND
  b) The information is confidential and ASX has not formed the view that the information has ceased to be confidential; AND
  c) A reasonable person would not expect the information to be disclosed.
- Given the very public nature of cyber attacks and the public scrutiny they now attract (and resulting impact on share price), there is an argument to say that the default should be that these attacks should be disclosed unless there is reason to believe otherwise. This is particularly so in light of Medibank's half yearly report which has stated the breach will cost between $40 million and $45 million – and this is excluding further potential customer and other remediation, regulatory or litigation related costs.
- It is rare that an organisation is immediately aware of the full scale and impact of a particular cyber incident. Investigations into these attacks are often extremely complex and are taking place as the business is trying to recover its system and serve its customers. The size and scale of the attack only becomes apparent sometime after discovery of the intrusion. The question arises as to when the appropriate time to inform the market as to the circumstances of the cyber attack.



10
My Health Records Act 2012 (Cth) – Notification of data breaches

Summary: Certain entities have mandatory obligations to provide notification of certain data breaches, including potential breaches, to the OAIC in connection with the My Health Record System.

Source?
My Health Records Act 2012 (Cth) s 75

Regulator?
Office of the Australian Information Commissioner **(OAIC)**

Who to notify?

- The OAIC
- The System Operator (currently, the Australian Digital Health Authority (ADHA))

Note: Affected individuals are notified by the System Operator (and not the entities who held the data).

Who needs to notify?

- Registered healthcare provider organisations;
- Registered repository operators;
- Registered portal operators; and
- Registered contracted service providers

When to notify?

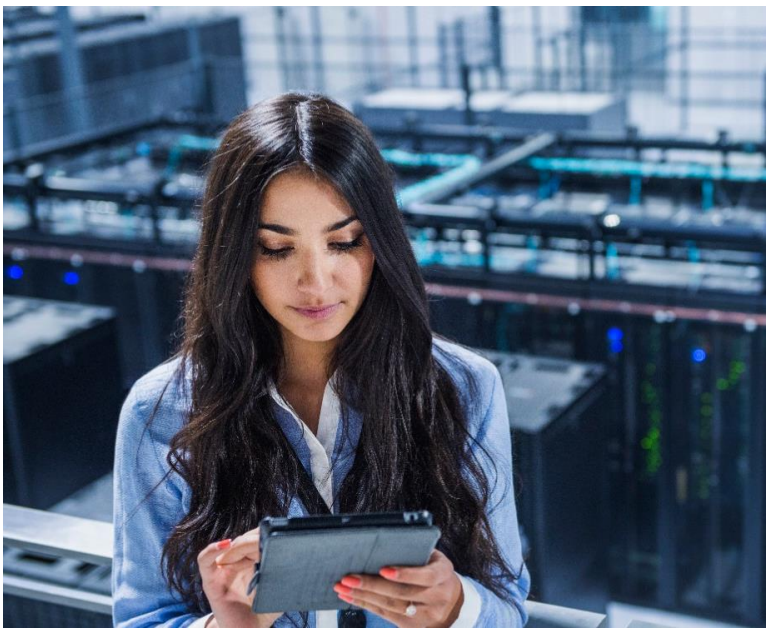
As soon as practicable after becoming aware of an eligible data breach.

Trigger for notification

An entity must notify the OAIC and System Operator where it becomes aware of:

a) the unauthorised collection, use or disclosure of health information in an individual's My Health Record in contravention of the *My Health Records Act 2012*; OR

b) an event or any circumstances that has, or may have, occurred or arisen that compromises, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system (whether or not involving a contravention of the *My Health Records Act 2012*).



Notice contents

The notification should include (where applicable):

- Contact details of the appropriate person within your entity
- A description of the data breach
- Date and time of the data breach
- Cause or potential cause of the data breach (whether inadvertent or intentional)
- Type of information involved
- Number of healthcare consumers that have or may have been affected.
- When and how you became aware of the breach
- Whether the data breach has been contained
- Any action taken or being taken to mitigate the impact of the data breach
- Any other relevant information

Additional notification details (can be added if desired):

- Whether the data breach appears to stem from a systemic issue or an isolated trigger
- Any other entities involved
- Whether your organization has experienced a similar breach in the past
- Any measures that were already in place to prevent the breach
- Whether a data breach response plan was in place and if it has been activated

Notice form

Eligible data breaches are reported to the OAIC through the online notification portal at https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion

Entities must also notify and provide the same incident details to the System Operator i.e., ADHA here.

Key considerations

- Because the System Operator is responsible for notifying those healthcare recipients affected by a confirmed notifiable data breach and those that would be affected by a potential notifiable data breach IF:

  a) there is a reasonable likelihood that the data breach occurred,

  b) and the effects might be serious for at least one healthcare recipient,

  then the entity must ask the System Operator to notify accordingly. Appropriate steps must be taken to ensure that appropriate communication is maintained between the System Operator and the entity. The System Operator must be aware of all facts and details of the breach and must be kept aware of any changes or developments in relation to the breach.
- Asking the System Operator to notify affected healthcare recipients is a separate step to reporting the notifiable data breach and, where this is required, must be carried out as soon as practicable after becoming aware of the breach.
- The OAIC recognises that some information about the breach may not be available when an initial report is made. This should not delay reporting, as further information can be provided when it becomes available.
- Any steps taken by the entity to rectify or contain the breach do not relieve the entity of its reporting obligations.

11
Privacy and Personal Information Protection Act 1998 (NSW) – Notification of eligible data breach

Summary: There is a mandatory obligation on State-owned corporations and public sector agencies to notify the NSW Privacy Commissioner and individuals of an eligible data breach. This obligation will come into effect on 28 November 2023.

Source?
Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW)

Regulator?
NSW Privacy Commissioner

Who to notify?

- The NSW Privacy Commissioner
- Affected individuals (being those individuals who would likely suffer serious harm as a result of their information being affected by the data breach)

Who needs to notify?

- NSW agencies; and
- NSW state owned corporations that are not covered by Commonwealth privacy law.

When to notify?

- Immediately notify the Privacy Commissioner.
- Where a data breach is only suspected, the agency has 30 days to assess the breach. The Privacy Commissioner must be notified of any extension to the assessment period.
- Individuals must be notified as soon as practicable

Trigger for notification

An agency must give a notification if the head of the public sector agency decides that:

a) An eligible data breach occurred; or

b) There are reasonable grounds to believe that the data breach is an eligible data breach.

An **eligible data breach** means—

a) there is unauthorised access to, or disclosure of, personal information held by a public sector agency which would likely result in serious harm to an individual to whom the information relates, or

b) personal information held by a public sector agency is lost in circumstances where—

   i. Unauthorised access to, or disclosure of, the information is likely to occur, and

   ii. If the unauthorised access to, or disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

Notice contents

The notification form, once published on the Information Privacy Commission's website, is likely to include:

- A description of the breach (including date of breach, how breach occurred, actions taken to mitigate the breach, etc.)
- A description of the personal information involved in the breach
- Whether the head of the agency is reporting on behalf of other agencies involved, and the details of the other agencies
- Whether the breach is a cyber incident, and details of the cyber incident
- The estimated costs of the breach to the agency
- The total or estimated number of individuals affected, or likely to be affected by the breach, and notified of the breach
- Whether the individuals notified have been advised of the complaints and internal review procedures under the Act

Notice form

The mandatory data breach notification form will be available on the Information and Privacy Commission's website – it has not yet been published.

The voluntary data breach notification form can be found on the IPC website.

Key considerations

- This amendment to the PPIP Act gives agencies a 12-month transition period to prepare appropriate systems and processes to fulfil new compliance obligations.
- The assessment of 'serious harm' to qualify an 'eligible data breach' has yet to be tested by the NSW Information and Privacy Commission. However, it is expected that the Commissioner will develop guidance, including key threshold questions, to assist agencies in assessing whether a data breach would be likely to result in serious harm to an individual.
- There are exemptions from mandatory notification in particular circumstances such as: where multiple public sector agencies are affected, where ongoing investigations and certain proceedings could be prejudiced, where notification is inconsistent with secrecy provisions, poses a serious risk to health and safety, and where cyber security could be compromised.
- Similarly, public sector agencies are exempt from notifying individuals of the data breach if an appropriate level of action has been taken to mitigate any serious harm to the individual. It remains to be seen what types of actions satisfy this exemption.
- Where agencies are unable to notify each individual or it is not reasonably practicable to do so, the agency must issue a public notification e.g. notice on a webpage or an announcement on social media pages.
- Where breaches involve a service provider that is an 'APP entity' (under the *Privacy Act 1988* (Cth)), agencies will need to ensure that their contracts address both state and Federal notification regimes.

12

Victorian Protective Data Security Standards – Information security incident notification

Summary: The information security incident notification scheme requires Victorian public sector agencies or bodies to notify OVIC of incidents that **compromise the confidentiality, integrity or availability of public sector information** that have been security assessed as having a 'limited' business impact or higher on government operations, organisations, or individuals

Source?
Element E9.010 of the Victorian Protective Data Security Standards
OVIC Information Security Incident Notification Scheme V1.0

Regulator?
Office of the Victorian Information Commissioner (OVIC)

Who to notify?

- OVIC

Who needs to notify?

- Victorian public sector (**VPS**) agencies or bodies.

When to notify?

- As soon as practical and **no later than 30 days** once an incident has been identified.

Trigger for notification

VPS organisations are required to notify OVIC of any compromise of public sector information that may cause '**limited**' (Business Impact Level 2) **or higher harm/damage** to government operations, organisations, or individuals.

'**Limited impact**' means a compromise of information which would be expected to cause limited harm or damage to government operations, organisations, or individuals.

Refer to the current Business Impact Level table for further information.

Notice contents

OVIC has identified some key fields for organisations to consider when submitting their notification, including:

- General details about the organisation and contact details
- Details about the incident, including date and time of occurrence, type of information affected, type of incident and what security attribute was affected (e.g. confidentiality, integrity, availability) and impacted security area (e.g. information, personnel, ICT/cyber or physical)
- Highest BIL of the affected information
- Business impacts as a result of the incident
- Steps taken or proposed to contain the incident
- Steps taken or proposed to prevent future incidents
- Whether incident response from the Cyber Incident Response Service (CIRS) or OVIC is required
- Whether the incident has been recorded in the organisation's incident register
- Whether the incident has been closed

Notice form

Incidents can be reported in writing via completing an incident notification form (available online at https://ovic.vic.gov.au/privacy/resources-for-organisations/information-security-and-privacy-incident-notification-form/).

Once the form is completed, email the form to incidents@ovic.vic.gov.au.

Where content of the incident is classified as PROTECTED or above, contact OVIC for further advice.

Incidents can also be reported orally to 1300 00 OVIC, although written reports are preferred

Key considerations

- Unlike the NSW regime which aligns with the *Privacy Act 1988* (Cth), the notification regime under the Victorian Protective Data Security Standards aligns more closely with ISO/IEC 27001 and the EU GDPR.
- Agencies or bodies need to consider the classification of any compromised information when determining how it responds to a cyber incident and how it engages with OVIC.
- OVIC may issue a notice to a non-compliant agency or body requiring the agency or body to take specific action in order to comply with the Standards. Failure to undertake these prescribed actions will result in monetary penalties being applied.
- Where breaches involve a service provider that is an 'APP entity' (under the *Privacy Act 1988* (Cth)), agencies will need to ensure that their contracts address both state and Federal notification regimes.

13
Australian Capital Territory

Summary: As at the time of publication, there are no mandatory cyber security incident/data breach notification requirements under ACT law.

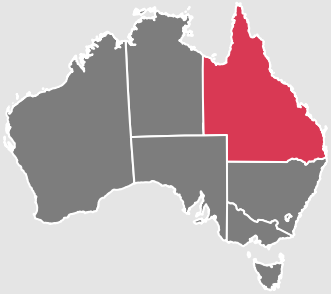
Key considerations

- ACT agencies can voluntarily notify the Office of the Australian Information Commissioner (**OAIC**) of a data breach. Under the OAIC's Memorandum of Understanding with the ACT Government, the OAIC will register any breaches notified by ACT agencies and provide further advice. Provision of advice or further services will be at the OAIC's discretion.

14

Queensland government enterprise architecture – Information security incident reporting

Summary: All Queensland government departments and some government bodies (e.g. statutory bodies) must apply the Queensland Government Enterprise Architecture (QGEA), which requires them to report certain information security incidents to the Queensland Government Chief Information Office (QGCIO).



Source?
Financial and Performance Management Standard 2019 under the Financial Accountability Act 2009 (Qld)
QGEA – Information Security Incident Reporting Standard (under the Information Security Policy (IS18:2018))

Regulator?
QGCIO

Who to notify?

- QGCIO

Who needs to notify?

- Queensland Government departments (as defined by the *Public Service Act 2008* (Qld))
- Accountable officers (not already in scope of the *Public Service Act 2008* (Qld)) and statutory bodies under the *Financial and Performance Management Standard 2019* (Qld) must have regard to the QGEA principles in the context of internal controls, financial information management systems and risk management

When to notify?

Immediately for security incidents affecting:

- A system with a Medium Business Impact Level (**BIL**) or above; or
- Multiple systems/departments

Quarterly for all other security incidents

Trigger for notification

Departments must report:

- Security incidents affecting a system with a **Medium BIL** or above;
- Security incidents affecting **multiple systems**/ departments; and
- **All other** security incidents.

'**Medium' BIL** means the information is sensitive. Sensitive information requires additional handling care due to its sensitivity or moderate business impact if compromised or lost.

BILs are defined in the Queensland Government Information Security Classification Framework and are determined by the business owner of the system.

Notice contents

The notification **must** include

- The affected organisation's contact information
- Details of the breach (including date and time discovered, scope of the incident, impact level on the business, details of the incident, indicators of compromise, and impact to the department)

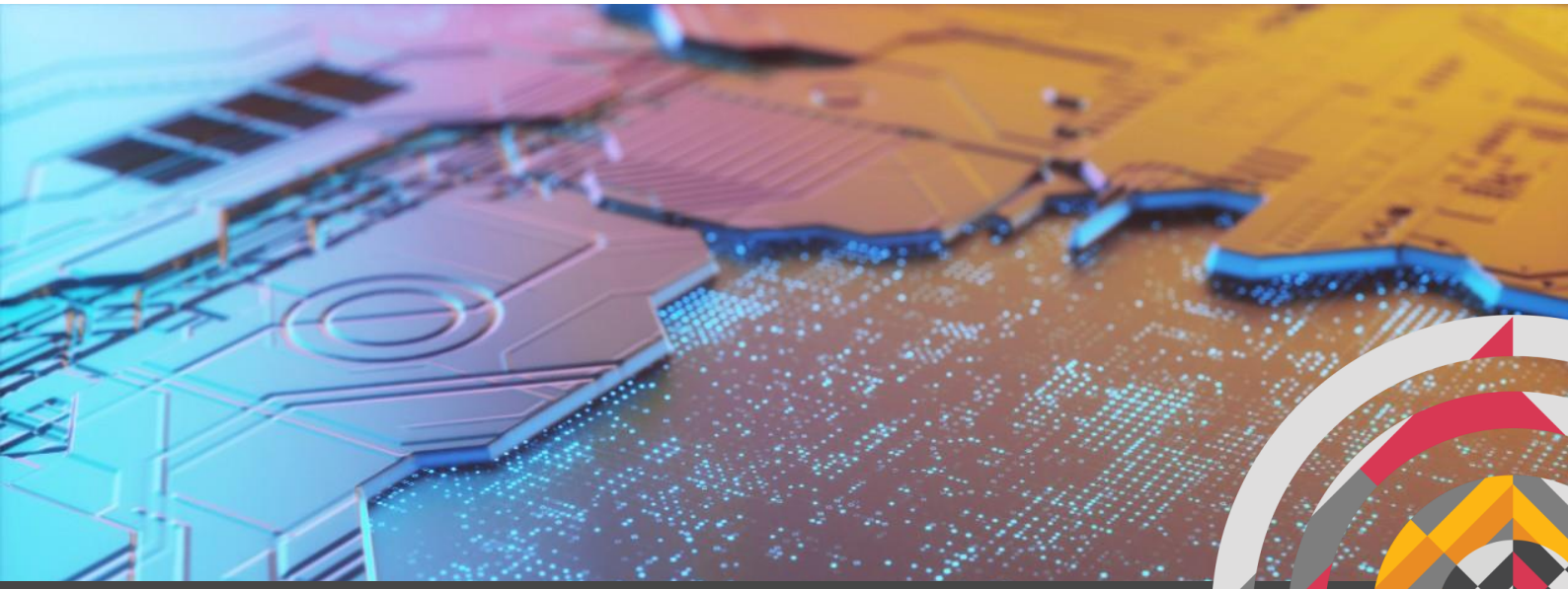
The notification **should** include any other fields defined in the Information security incident reporting spreadsheet.

Quarterly reports should also include a copy of the department's information security incident register.

Notice form

For **immediate** reporting, departments can notify via phone on 07 3215 3951, email at qgisvrt@qld.gov.au, or any other formally agreed upon channel.

For **quarterly** reporting, departments must submit the report no later than two weeks after the final day in each quarter via email to qgisvrt@qld.gov.au.



Key considerations

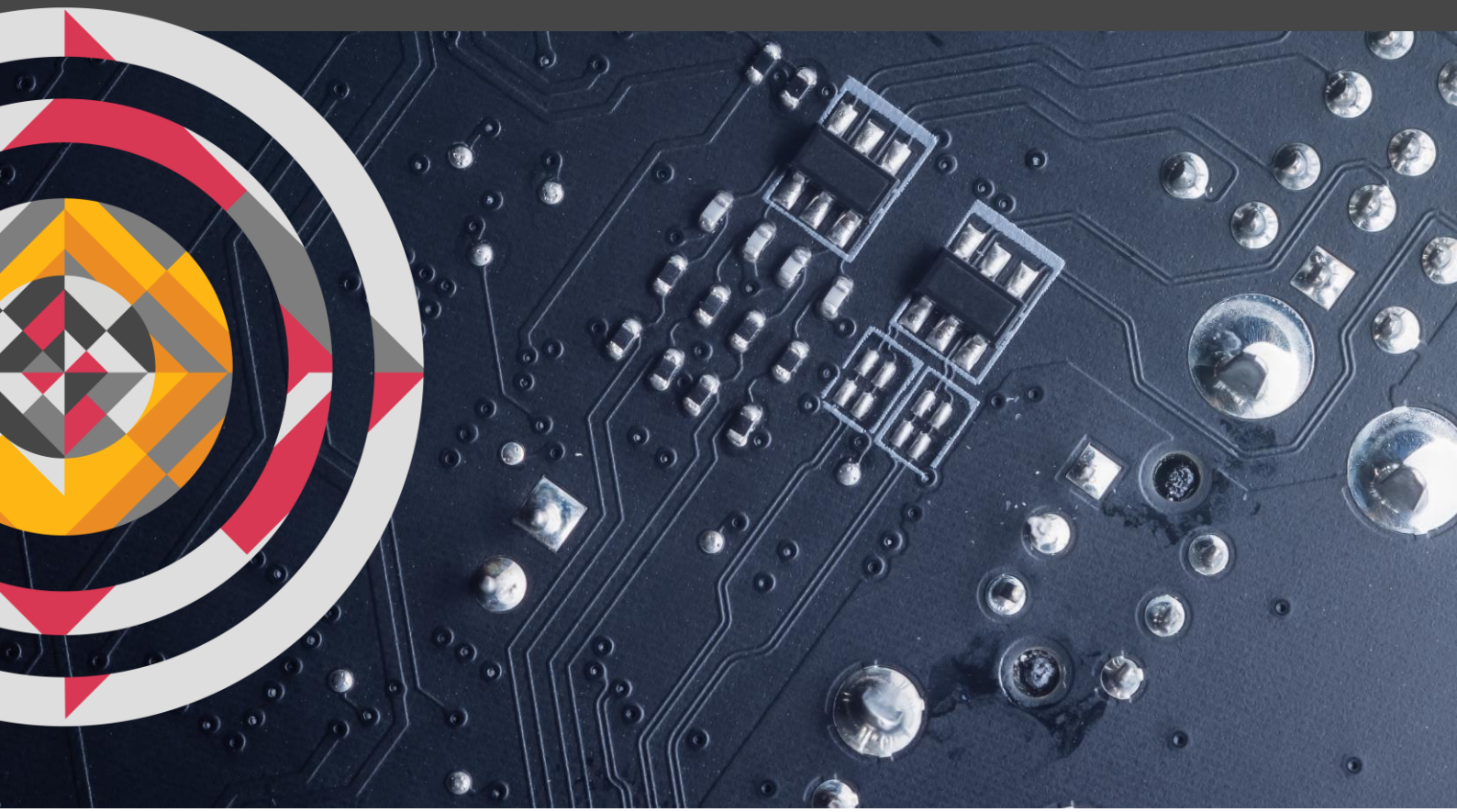
- The requirement to notify under the Queensland regime is enlivened under the Financial and Performance Management Standard 2019 (which is made under the *Financial Accountability Act 2009* (Qld)) rather than the state-based *Information Privacy Act 2009* (Qld).
- Unlike Victoria and NSW, this regime is not centred around personal information held by government bodies, rather it is focussed on disruption to government functions e.g. internal financial controls.
- The Information Security Policy (IS18:2018) is based upon the ISO/IEC 27000 and the Information Security Incident Management Policy is based upon ISO/IEC 27035.
- The OIC in Queensland strongly encourages Queensland government bodies to voluntarily notify the OIC given that the OIC is able to provide advice on responding to the breach, and further assist the OIC in responding to community queries in relation to the breach.
- The OIC also recommends notifying affected individuals in appropriate circumstances (it is important to note that the OIC considers **any** risk of harm to an individual a reason to notify that individual cf. a risk of serious harm at the Federal level). The OIC provides a privacy breach self-assessment tool to assist in assessing harm to individuals as a result of the breach.

15
Northern Territory

Summary: As at the time of publication, there are no specific mandatory cyber security incident/data breach notification requirements under Northern Territory law.

Key considerations

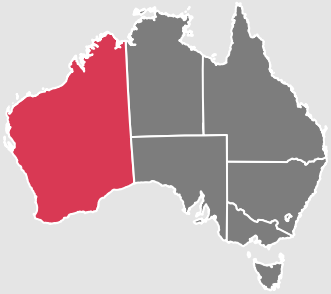
- It is possible that the existence of a data breach may constitute 'government information' that should be shared with individuals under s 10(1) of the Information Act 2002 (NT), which requires public sector organisations to proactively make available to the public any such government information promptly and as is reasonably possible.



16

Western Australian whole-of-government cyber security incident coordination framework – Reporting cyber security incidents

Summary: Under the framework, agencies must report cyber security incidents to the Office of Digital Government and the WA Police Force's Technology Crime Services.



Source?
Western Australian Whole-of-Government Cyber Security Incident Coordination Framework

Regulator?
- Office of Digital Government
- WA Police Force's Technology Crime Services

Who to notify?

- Office of Digital Government
- WA Police Force's Technology Crime Services

Who needs to notify?

- Departments, SES and non-SES organisations as defined in the Public Sector Management Act 1994 (WA)
- Western Australian Police Force
- Entities contracted as Managed Service Providers (**MSPs**) of the GovNext Core
- Entities contracted as MSPs for agencies consuming GovNext Services

When to notify?

Unable to be determined.

We note that *only* state government organisations can contact the Cyber Security Unit to request the framework by emailing cybersecurity@dpc.wa.gov.au.

Trigger for notification

Unable to be determined.

Notice contents

Unable to be determined.

Notice form

Western Australia Government Agencies can report a cyber security incident on the reporting portal.

Key considerations

- The Western Australian Whole-of-Government Cyber Security Incident Coordination Framework is established under a Circular, and therefore the notification obligations are not a requirement under a formal legislative instrument. However, it is likely that general administrative laws will apply, and relevant entities would be expected to act in compliance with the Framework regardless.
- Accordingly, it is unclear what the specific ramifications are for non-compliance with the Framework.

17

Government of South Australia, premier and cabinet circular PC042 cyber security incident – Reporting cyber security incidents

Summary: South Australian **(SA)** Government public sector agencies and suppliers and non-government personnel providing services to SA Government must report cyber security events and incidents to the Control Agency for Cyber Crisis in accordance with PC042 Cyber Security Incident and Guideline 4.0: Cyber security event and incident reporting of the South Australian Cyber Security Framework **(SACSF).**

Source?
PC042 Cyber Security Incident Management
SACSF Guideline 4.0: Cyber security event and incident reporting

Regulator?
Control Agency for Cyber Crisis (currently, the Department of the Premier and Cabinet (DPC))

Who to notify?

- Control Agency for Cyber Crisis (currently, the DPC) via the Watch Desk.

Who needs to notify?

- All SA Government public sector agencies (as defined in the Public Sector Act 2009 (SA))
- Suppliers and non-government personnel providing services to SA Government.

When to notify?

A report should be immediately provided to the Control Agency.

Trigger for notification

Where an agency or supplier has identified a cyber security event, or otherwise suspects a cyber security incident has occurred, they must notify the DPC.

Cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards, or a previously unknown situation that may be relevant to security.

It is irrelevant whether the attack/event is successful or whether there are any consequences for SA Government information or cyber assets.

Cyber security incident is a single or series of unwanted or unexpected events that impact the confidentiality, integrity or availability of a network or system or the information it stores, processes or communicates.

These should be reported even if their impact is minimal e.g. unexplained outages or data breach.

Notice contents

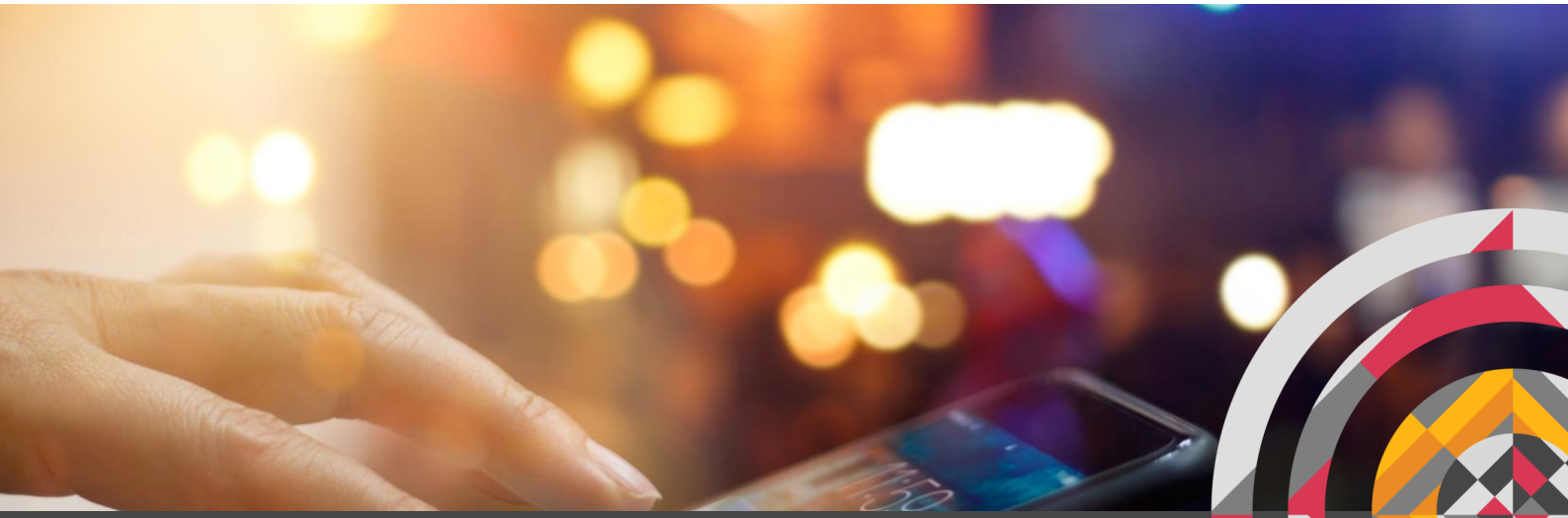
Where possible, the following information should be included when making a report:

- the date and time the cyber security incident occurred;
- the date and time the cyber security incident was discovered;
- a description of the cyber security incident;
- any actions taken in response to the cyber security incident;
- to whom the cyber security incident was reported; and
- if assistance is required for incident response.

Notice form

A report may be submitted by whomever the agency considers appropriate to do so. This may be a cyber security officer, ICT support officer or service desk personnel.

Reports can be made either orally to 1300 244 168 (Press 2), or in writing via email to: watchdesk@sa.gov.au.



Key considerations

- SA's Watch Desk will notify the Australian Cyber Security Centre **(ACSC)** regarding cyber security incidents. It is the single point of contact between SA Government public sectors agencies (and its suppliers/non-governmental personnel suppliers) and the ACSC. Agencies do not need to independently report cyber security incidents to the ACSC.
- Where illegal activity is involved during a cyber security incident, a report must also be made the SA Police.
- Given the different documents outlining cyber security incident reporting requirements, it is important to ensure entities are aware of changes or amendments to its obligations in any of the documents.
- The SA notification requirements are established under a Circular, and therefore the notification obligations are not a requirement under a formal legislative instrument. However, it is likely that general administrative laws will apply, and relevant entities would be expected to act in compliance with the Circular regardless.
- Accordingly, it is unclear what the specific ramifications are for non-compliance with the Circular.
- Should there be a declaration of an emergency under the *Emergency Management Act* 2004 (SA), the powers and functions of authorised officers under that Act would supersede those assumed under this Circular.

18

Tasmanian government incident management cybersecurity standard – Notification of cybersecurity events and incidents

Summary: Agencies have an obligation to report suspected or confirmed cybersecurity events or incidents (as defined in the Tasmanian Government Incident Management Cybersecurity Standard) in a timely manner.

Source?
Tasmanian Government Incident Management Cybersecurity Standard
Tasmanian Government Cybersecurity Incident Management Arrangements

Regulator?
Tasmanian Government Chief Information Officer **(TGCIO)**

Who to notify?

- TGCIO

Who needs to notify?

- All Tasmanian Government agencies as listed in Schedule 1 of the *State Service Act 2000* (Tas).

** Other Tasmanian Government organisations may choose to notify.*

When to notify?

Notification should be made in a **timely** manner. Specific requirements may be contained in the Tasmanian Government Cybersecurity Incident Management Arrangements.

We note that *only* state government organisations can access this document by contacting the Department of Premier and Cabinet.

Trigger for notification

Tasmanian Government agencies must notify of suspected or confirmed cybersecurity events and incidents which could impact public confidence or affect delivery of government services..

Cybersecurity events are identified occurrences of a system, service or network state indicating a possible breach of information security policy or failure of safeguards; or a previously unknown situation that may be security relevant.

Cybersecurity incidents are a single or series of unwanted or unexpected cybersecurity events that have a significant probability of compromising business operations and threatening information security.

Notice contents

Agencies are to notify as per the Tasmanian Government Cybersecurity Incident Management Arrangements.

We note that *only state government organisations* can access this document by contacting the Department of Premier and Cabinet.

Notice form

Cyber security incidents can be reported in writing via email to: cybersecurity@dpac.tas.gov.au.

Key considerations

- The Tasmanian Government standards attempt to provide a consistent, systematic and repeatable approach enabling collaboration across government and the private sector. It aligns itself with ISO/IEC 27001 for cyber security management requirements.
- The notification obligations under the Tasmanian Government Incident Management Cybersecurity Standard are not a requirement under a formal legislative instrument. However, it is likely that general administrative laws will apply, and relevant entities would be expected to act in compliance with the Standard regardless.
- Accordingly, it is unclear what the specific ramifications are for non-compliance with the Standard.

19
Our team and how we can help

Our team and expertise

The PwC Digital, Cyber and Technology Legal team has extensive experience advising clients on all aspects of preparing for and responding to cyber security incidents and data breaches. From first detection of intrusion, dealing with regulators and key stakeholders through to managing insurance claims under cyber policies after the recovery and investigation is complete. Our team works hand in glove with our security and risk professionals within the firm to provide a multi-disciplinary and fully integrated response to cyber incidents.

Further, PwC has helped hundreds of Australian organisations improve their cyber resilience and response capabilities and are well placed to assist you in facilitating a Data Breach Readiness assessment for your organisation. PwC has a range of standard solutions to assist you with carrying out this assessment and should bespoke services be required, we have procedures that can be undertaken to rapidly improve your data breach response capability.

How we can help

We have all of your digital, cyber and technology needs covered and we leverage our network to provide an integrated solution across the following areas of expertise:

- Technology transformation, outsourcing and large scale strategic procurement
- The internet of things
- Intellectual property and software licensing
- Complex commercial arrangements and M&A transactional support
- Emerging technologies: Artificial intelligence, blockchain & robotics
- Data: Date protection, analytics, commercialisation & privacy
- Agile and output based contracting
- Telecommunications services and technology infrastructure
- Cyber security: Security of critical assets and incident response
- Cloud contracting and ‘as a service’ sourcing models

20
Key contacts

Please contact any of our team listed below to discuss how PwC can assist you in relation to your incident response processes and procedures, including in relation to:

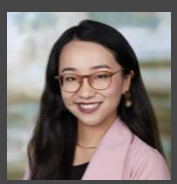
- data breach and cyber incident readiness assessments;
- compliance maturity assessments; and
- all aspects of responding to cyber incidents.

Adrian Chotar
Partner | Head of Digital, Cyber and Technology Law
PwC Australia
T: +61 (0)457 808 068
E: adrian.chotar@au.pwc.com

James Patto
Director | Digital, Cyber and Technology Law
PwC Australia
T: +61 (0)431 275 693
E: james.patto@au.pwc.com

Authors and contributors

James Patto
Director | PwC Australia
Digital, Cyber & Technology Law



Annie Zhang
Associate | PwC Australia
Digital, Cyber & Technology Law

Elsa Zhong
Lawyer | PwC Australia
Digital, Cyber & Technology Law

We would also like to express our thanks to Arsh Rampal and the PwC Australia 2022-23 summer clerks, Avishay Kumar, Vannia Coquis Morales, Olivia Sasse and Tiffany Zwanink, for their assistance and contribution to this publication.

A community of solvers coming together in unexpected ways to solve the world's important problems

www.pwc.com.au

© 2023 PricewaterhouseCoopers. All rights reserved. PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Liability limited by a scheme approved under Professional Standards Legislation. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.
PWC200793448