

INTERNAL

## Standard operating procedure

### Access to telecommunication data under the *Telecommunications (Interception and Access) Act 1979*

<b>Published date:</b>	11/08/14
<b>Availability:</b>	Limited
<b>Purpose:</b>	To guide the request, authorisation, receipt, use, recordkeeping and reporting requirements for telecommunications data obtained under the <i>Telecommunications (Interception and Access) Act 1979</i> .
<b>Owner:</b>	Manager, Intelligence & Analytics
<b>Category:</b>	Investigations and enforcement
<b>Sub-category:</b>	Agency relationships
<b>Contact:</b>	██████████ x ██████ )

# Contents

Standard operating procedure .....	1
Access to telecommunication data under the <i>Telecommunications (Interception and Access) Act 1979</i> .....	1
Contents .....	2
Introduction.....	3
Definitions .....	4
Scope.....	5
Responsibilities .....	6
Standard operating procedure .....	6
Overview .....	6
Lawful access to telecommunications data: .....	7
1. Lawful access to telecommunications data .....	8
1.1. Requesting the disclosure of telecommunications data .....	8
1.2. Authorising the disclosure of telecommunications data .....	11
1.3. Notifying a carrier or carriage service provider of an authorisation ....	12
1.4. Receiving telecommunications data.....	14
2. Use of telecommunications data.....	15
2.1. Use of telecommunications data.....	15
3. Recordkeeping and Reporting.....	15
3.1. Recordkeeping.....	15
3.2. Reporting .....	16
Legislative framework .....	17
Related policies and references.....	17
Chief Executive Instructions .....	17
Policies .....	17
Other references.....	17
Consultation.....	18
Endorsement .....	18
Approval .....	18
Version control.....	18
Appendix A: Enforcement agency – Authorisation and notification for access to existing information or documents .....	20
Appendix B: List of authorized officers .....	3

### Summary of main points

This Standard Operating Procedure is intended to guide the request, authorisation, receipt, use, recordkeeping and reporting requirements for telecommunications data obtained under the *Telecommunications (Interception and Access) Act 1979*.

This standard operating procedure applies to staff responsible for accessing telecommunications data for the purposes of:

- the enforcement of the criminal law; and
- the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Unless specifically authorised otherwise by the Chief Executive Officer or an authorised officer within the meaning of section 5 of the *Telecommunications (Interception & Access) Act 1979*, this Standard Operating Procedure constitutes a direction within the meaning of the Code of Conduct in the *Public Service Act 1999*.

## Introduction

This Standard Operating Procedure sets out how to access telecommunications data under the *Telecommunications (Interception & Access) Act 1979* (the TIA Act).

The TIA Act provides mechanisms for enforcement agencies to authorise carriers to disclose information or documents in particular circumstances. Information or documents in this context are known as ‘telecommunications data’.

The Clean Energy Regulator (CER) is an enforcement agency under the TIA Act. While recognising the usefulness of telecommunications data as an enforcement tool, the CER appreciates the potential sensitivity of information source and the legislative provisions in place to maintain integrity. In order to meet its legislative obligations, the CER will limit access to telecommunications data and establish robust mechanisms for requesting, accessing and using this data.

These SOP underpin this broad approach and seeks to ensure that CER staff can meet their statutory obligations under the TIA Act.



## Definitions

Term	Definition
Authorisation form	Documentation authorising disclosure of telecommunications data in line with the requirements of s. 183 of the TIA Act. The Authorisation form may also constitute a notification under the TIA Act.
Authorised officer	<p>An 'authorised officer' is defined in section 5(1) of the TIA Act as being the head, deputy head or a person who holds or is acting in a management office or position in the enforcement agency that is covered by an authorisation under subsection 5AB(1) of the TIA Act.</p> <p>Positions covered by an authorisation under subsection 5AB(1) of the TIA Act in the CER are listed in Appendix B on this SOP.</p>
Enforcement agency	is defined in s.5 of the TIA Act and includes a body whose function includes administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.
Historical telecommunications data	Telecommunications data that is already in existence at the time of the request for access to that data.
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity (IMSI)
IPND	Integrated Public Number Database
Notification	Section 184 of the TIA Act provides that an employee of the enforcement agency must notify the person from whom the data was sought of an authorisation or revocation. Carriers operate on the <i>notification</i> , not the authorisation, and it is the notification that gives rise to the disclosure of information. A single document can constitute both an authorisation and notification providing that it complies with the requirements of both.
Relevant staff member	Defined in the TIA Act (subsection 5(1)) as the head of an agency, a deputy head of an agency or any employee, member of staff or officer of the enforcement agency. A relevant staff member of an enforcement agency is authorised to notify a carrier or carriage service provider of the making of an authorisation for the disclosure of historical or prospective telecommunications data.



Requesting officer	An officer within the Investigations and Enforcement Branch or the Intelligence and Analytics Section of the CER that seeks to initiate a lawful request for the disclosure of telecommunications data under the TIA Act.
Telecommunications data	includes information about a telecommunication that does not reveal the content or substance of a telecommunication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet-based applications including internet browsing and voice over internet telephony. For telephone-based communications, telecommunications data includes: <ul style="list-style-type: none"> <li>• Subscriber information</li> <li>• The telephone numbers of the parties involved</li> <li>• The time of the call and its duration.</li> </ul> In relation to internet-based applications, telecommunications data includes the Internet Protocol (IP) address used for the session and the start and finish time of each session.
TIA Act	<i>Telecommunications (Interceptions and Access) Act 1979</i>

## Scope

This Standard Operating Procedure applies to requests for the disclosure of telecommunication information from carriers in particular circumstances. As an enforcement agency under the TIA Act, the CER is able to request telecommunications information where it is reasonably necessary for:

- The enforcement of the criminal law (section 178 of the TIA Act);
- The enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (section 179 of the TIA Act).

This Standard Operating Procedure sets out the mandatory procedures for:

- authorising the disclosure of telecommunications data by authorised officers within the CER
- recordkeeping in relation to authorisations under the TIA Act.
- reporting requirements under the TIA Act.

This Standard Operating Procedure also operates as a direction to officers for the purposes of the APS Code of Conduct and the *Public Service Act 1999*. Unless specifically authorised otherwise by **the Chief Executive Officer** or an authorised officer within the meaning of section 5 of the Telecommunications (Interception & Access) Act 1979, staff must comply with this Standard Operating Procedure.

Telecommunications data is an important source of information for investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest. In simple investigations telecommunications data is used to provide information or evidence directly related to the investigation. In complex investigations telecommunications data is used to build a picture of suspected offences by identifying participants, establishing relationships and levels of contact.

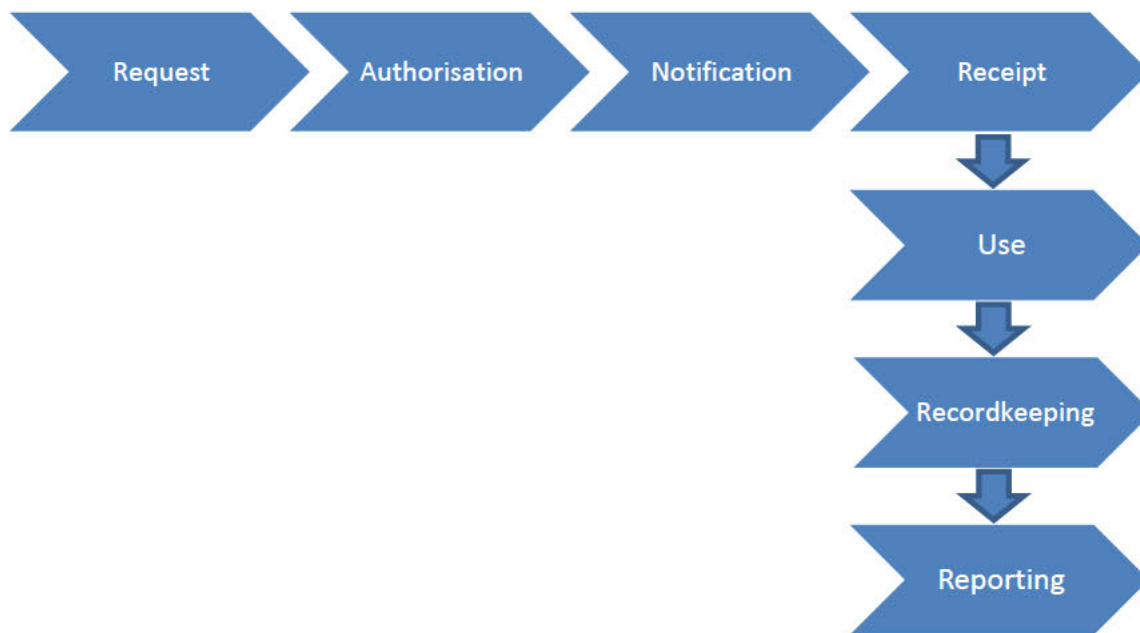
## Responsibilities

Person/position/team	Responsibility
Authorised officers	<p>They authorise the disclosure of telecommunications information under Chapter 4 of the TIA Act. Under the direction under s5AB of the TIA Act, only the Chair and Chief Executive Officer has been authorised the disclosure of telecommunications data.</p> <p>Positions covered by an authorisation under subsection 5AB(1) of the TIA Act in the CER are listed in Appendix B on this SOP.</p>
Chief Executive Officer	In addition to authorising disclosure of telecommunication data, approves other management positions within the CER as authorised officers for the purpose of accessing telecommunications information under the TIA Act.
Relevant staff member	CER staff member that is authorised to notify a carrier or carriage service provider of the making of an authorisation for the disclosure of telecommunications data.
Requesting officer	A CER officer who wishes to access telecommunications data for the purposes of enforcing the criminal law or the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

## Standard operating procedure

### Overview

The process to seek a disclosure of telecommunications data is a four-step process (from request, to authorisation, to notification, and receipt). Following disclosure, there are also processes that must be adhered to relating to the use, recordkeeping and reporting of telecommunications data. This process is illustrated in the flow chart below.

**Lawful access to telecommunications data:**



# 1. Lawful access to telecommunications data

## 1.1. Requesting the disclosure of telecommunications data

- 1.1.1. A request for the disclosure of telecommunications data under the TIA Act can be initiated by any staff member of the Investigations and Enforcement Branch or the Intelligence and Analytics Section. This staff member is referred to as the “requesting officer”.
- 1.1.2. A request for the disclosure of telecommunications data must be in support of an existing CER case or investigation, and must be reasonably necessary for the enforcement of the criminal law or the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.
- 1.1.3. To maintain integrity and protect evidence, a requesting officer cannot be the same person as the authorised officer authorising the request. An authorised officer that seeks to request telecommunications data for investigative purposes should submit their request to another authorised officer within the agency to get an authorisation for the disclosure of that information, being a person who is separate from the investigation itself.
- 1.1.4. Requesting officers can seek to request the disclosure of specified information or specified documents that are in existence at the time of the request the request is made. Specified information or specified documents may take many forms, and will vary depending on the carrier or carriage service provider, but will generally take the form of one or more of the following:
  - Subscriber details
  - Integrated Public Number Database (IPND) Enquiry
  - Call Record Information, including:
    - » Fixed Service Call Records (ongoing calls)
    - » Fixed Call Records (incoming calls)
    - » Fixed Call Records (both incoming and outgoing calls)
    - » Mobile Service Call Records (ongoing calls)
    - » Mobile Call Records (incoming calls)
    - » Mobile Call Records (both incoming and outgoing calls)
  - International Mobile Equipment Identifier (IMEI)
  - Email address registration details
  - Mobile location Search

The type of specified information or specified documents that are available from different carriers or carriage service providers will vary, and the prices for disclosures will also vary. The Intelligence and Analytics Section will maintain a list of products available and associated pricing (with respect to the TIA Act) specific to different carriers.

- 1.1.5. Requesting officers must use the “Enforcement Agencies - Authorisation and notification for access to existing information or documents” template, provided in Appendix A, for any request for the disclosure of telecommunications data.
  - 1.1.5.1. For authorisations under section 178 of the TIA Act, the authorised officer must be satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law before they authorise the disclosure. In order to assist the authorised officer meet this threshold, the request for authorisation under s178 must be accompanied by relevant case notes or briefing material, and must cite the particular offence under CER legislation to which the disclosure relates.
  - 1.1.5.2. For authorisations under section 179 of the TIA Act, the authorised officer must be satisfied that the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue before they authorise the disclosure. In order to assist the authorised officer meet this threshold, the request for authorisation under s179 must be accompanied by relevant case notes or briefing material, and must cite the particular CER legislative provisions which appear to have been breached and the provision which imposes a pecuniary penalty
- 1.1.6. Requesting officers must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use of telecommunications data under request is justifiable, having regard to:
  - The likely relevant and usefulness of the information or documents;
  - The reason why the disclosure or use concerned is proposed to be authorised.
- 1.1.7. Requesting officers should ensure that any requests are specific to a particular person or particular investigation. Requesting officers



should ensure that authorisations do not authorise the disclosure of information that may be of interest in the context of other investigations.

While authorisations are not required to be targeted to a service, person or investigation, enforcement agencies should ensure that authorisations clearly identify which case or matter to which the request relates. The same authorisation cannot be applied to different investigations. This will assist in ensuring that information is not inadvertently required to be released in evidentiary processes and will assist with reporting requirements.

- 1.1.8. Requesting officers are responsible for seeking financial approval for lawful requests for the disclosure of telecommunication data in accordance with the *Public Governance, Performance and Accountability Act 2013*.
- 1.1.9. Requesting officers are responsible for ensuring that requests for the authorisation for disclosure of telecommunications data, using the form provided in Appendix A, is provided to an authorised officer within the agency and will work with the authorised officer to ensure that their legislative requirements under the TIA Act can be met. Positions covered by an authorisation under subsection 5AB(1) of the TIA Act in the CER are listed in Appendix B on this SOP.

Requesting officers are encouraged to seek assistance from the Office of the General Counsel in making requests to authorise the disclosure of telecommunications data under the TIA Act.

**AGD assistance**

Assistance relating to specific circumstances relating to telecommunications data can be obtained from the Telecommunications and Surveillance Law Branch of the Attorney-General's Department on telephone number (02) 6141 2900.



## 1.2. Authorising the disclosure of telecommunications data

- 1.2.1. Authorised officers in the CER are responsible for ensuring the authorisations for the disclosure of telecommunication data meet the legislative requirements of the TIA Act. A list of officers authorised by the Chair and Chief Executive Officer of the CER under s5AB of the TIA Act is provided in Appendix B.
- 1.2.2. Upon receipt of an “Enforcement Agencies - Authorisation and notification for access to existing information or documents” request, the authorised officer must:
  - Ensure that the proposed authorisation form is complete;
  - Ensure that:
    - » For proposed authorisations under section 178 of the TIA Act, the disclosure is reasonably necessary for the enforcement of the criminal law, and is accompanied by supporting case notes or briefing material to satisfy this requirement, including the particular offence under CER legislation for which the disclosure is sought.
    - » For proposed authorisation under section 179 of the TIA Act, the requesting officer must have regard as to whether the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue, and is accompanied by supporting case notes or briefing material to satisfy this requirement, and must cite the particular breaches or legislative references under CER legislation for which the disclosure is sought.
  - Have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use of telecommunications data under request is justifiable, having regard to:
    - » the likely relevance and usefulness of the information or documents;
    - » the reason why the disclosure or use concerned is proposed to be authorised.
  - Have regard to whether the requests are specific to a particular person or investigation.
  - Providing financial approval for lawful requests for the disclosure of telecommunication data in accordance with the *Financial Management and Accountability Act 1997*, *FMA Regulations* and *FMA Orders*.
- 1.2.3. Once the authorised officer is satisfied that the information provided on the “Enforcement Agencies - Authorisation and notification for

access to existing information or documents” request meets legislative requirement, the authorised officer may authorise the request by signing and dating the form.

- 1.2.4. Authorised officers must then provide the signed “Enforcement Agencies - Authorisation and notification for access to existing information or documents” form to a relevant staff member within the Investigation and Enforcement Section or Intelligence and Analytics Section to notify the relevant carrier or carriage service provider of the authorisation. The authorisation must also be provided to the Intelligence and Analytics Section to ensure that recordkeeping and reporting requirement of the TIA Act can be met.
- 1.2.5. The Authorised officer must also communicate to the relevant staff member any particular security requirements for the transfer of information to the carriage service provider.

### 1.3. Notifying a carrier or carriage service provider of an authorisation

- 1.3.1. The requesting officer and the relevant staff member can be the same person. The authorising officer can also be the same person as the relevant staff member.
- 1.3.2. In accordance with section 184 of the TIA Act, the relevant staff member must notify the person from whom the data was sought of an authorisation. The relevant staff member should communicate with the relevant carrier or carriage service provider to determine what mode of delivery is required or optimal. The relevant staff member should also determine what forms or template the carrier or carriage service provider prefers with regards to the notification. Should the carrier or carriage service provide require an alternative form or template to be used, the relevant staff member should transcribe the relevant information from the Enforcement agency – Authorisation and notification for access to existing information or documents Form to the carrier’s preferred template.

Carriers operate on the *notification*, not the authorisation, and it is the notification that gives rise to the disclosure of information.

The Enforcement agency – Authorisation and notification for access to existing information or documents Form constitutes both an authorisation and notification, as it complies with the requirements of both.<sup>1</sup>

<sup>1</sup> As at 26 June 2013.

- 1.3.3. The relevant staff member must comply with any particular security requirements for the transfer of information to the carriage service provider, either at the direction of the authorised officer or the carrier or carriage service provider.

Telecommunication data will be transmitted via secure means maintained by the Investigations and Enforcement Branch. This includes the management of a dedicated, secure fax machine to be used for this purpose.

- 1.3.4. After notifying the carrier or carriage service provider of the authorisation, the signed "Enforcement Agencies - Authorisation and notification for access to existing information or documents" form should be scanned and added to CER intelligence and/or investigative systems, including the following criteria:

- Document type (i.e. Telecommunications data authorisation)
- Document sub-type (i.e. s178 – Enforcement of the criminal law or s179 – Enforcement of a law imposing a pecuniary penalty or protection of the public revenue)
- Document title, which make include details of:
  - » the carrier
  - » the specified information or documents sought
  - » the person or telephone number to which the authorization relates
  - » the date period to which the authorisation relates (for call charge records)



Document title examples:

- Telstra subscriber check for 0261596666
- IPND check for Malcolm John SPARROW
- Optus call charge record for 0261597777 for date period 01/01/2013 to 31/03/2013

- The name of the authorising officer
- The date on which the authorisation was made.
- The file cover record in which the hard-copy authorisation record is maintained.

#### 1.4.Receiving telecommunications data

- 1.4.1. Telecommunications data will be received in the manner requested by the CER, or at the discretion of the carrier or carriage service provider. Telecommunications data will usually be received by the relevant staff member who notified the carriage service provider of the authorisation. Receipt of telecommunications data will always be limited to members of the Investigations and Enforcement Branch or the Intelligence and Analytics Section.
- 1.4.2. The staff member receiving the telecommunications data is responsible for notifying members of the investigative team that telecommunications data has been received. This will include:
  - The requesting officer
  - The authorising officer
  - The relevant staff member
- 1.4.3. After receiving the telecommunications data, the staff member will also update CER intelligence and/or investigative systems that the requested information has been received.

## 2. Use of telecommunications data

### 2.1. Use of telecommunications data

- 2.1.1. The use of telecommunications data as evidence is limited to the investigation for which it was first sought.
- 2.1.2. Telecommunication data can be added to CER intelligence holdings for future reference and to identify issues across investigations.
- 2.1.3. If telecommunication data obtained through an authorisation processes is relevant to another investigation or a separate matter, this information must be obtained again through an independent authorisation process.
- 2.1.4. Telecommunication information obtain under the TIA is considered to be “protected information” under the CER Act and will be managed in accordance with “Protected” security classified information under the Protective Security Policy Framework.

## 3. Recordkeeping and Reporting

### 3.1. Recordkeeping

- 3.1.1. Section 185 of the TIA Act stipulates that all authorisations are to be retained for a period of no less than 3 years. However, the CER will retrain records of authorisations for longer periods in accordance with the CER’s records management authority.
- 3.1.2. The CER’s Intelligence Database, maintained by the Intelligence and Analytics Section, is the primary system for recording and reporting authorisations made under the TIA Act. For this reason, all authorisations must be provided to the Intelligence and Analytics Section.
- 3.1.3. Authorisations should also be recorded in other relevant systems (including the Jade Case Management System and relevant case folders in shared drive (G: drive)). However, these systems will not serve to facilitate reporting.
- 3.1.4. The hard copy record of the authorisation must be retained in an appropriate file cover pertaining to the case. This will in general be maintained by the Investigations and Enforcement Branch. This is the official record for recordkeeping purposes. This file cover record number should also be recorded in the CER’s intelligence and/or investigative systems.

### 3.2. Reporting

- 3.2.1. Under s186 of the TIA Act, the CER is required to report annually (no later than within 3 months of the end of the financial year) to the Attorney-General regarding its access to telecommunications data. The CER's report must include statistics on the number of authorisations made during the previous financial year for:
- The disclosure under s. 178 of existing telecommunications data for the enforcement of the criminal law
  - The disclosure under s. 179 of existing telecommunications data for the purpose of enforcing a law imposing a pecuniary penalty or the protection of the public revenue
  - Any other matter requested by the Minister in relation to those authorisations.
- 3.2.2. The Attorney-General will then compile the reports of all enforcement agencies into an annual report for Parliament.
- 3.2.3. The Manager, Intelligence and Analytics Section, is responsible for preparing reports to the Attorney-General's Department under s186 of the TIA Act.
- 3.2.4. The Chief Investigations Officer is responsible for the approval and delivery of these reports to the Attorney-General's Department.



## Legislative framework

Reference	Section or regulation
<i>Public Governance, Performance and Accountability Act 2013</i>	
<i>Telecommunications (Interception and Access) Act 1979</i>	Section 5 Section 5AB(1) Section 178-186

## Related policies and references

### Chief Executive Instructions

- CEI 2 - Committing to spend public money
- CEI 3 – Procurement
- CEI 5 – Commonwealth credit cards and credit vouchers
- CEI 6 – Making payments of public money

### Policies

- CER Investigations manual
- Fraud Control Plan


### Other references

- Governance Framework for Addressing Non-Compliance and Fraud
- Telecommunications (Interception and Access) Act 1979 – Information Sheet No. 7 – Disclosure of Telecommunications Data


## Consultation

<b>Internal stakeholders:</b>	Chief Investigations Officer General Counsel
<b>External stakeholders:</b>	Australian Competition and Consumer Commission





## Endorsement

<b>Endorsed on:</b>	
<b>By:</b>	 Acting General Manager, Scheme Integrity and Carbon Information Branch
<b>Signature:</b>	

## Approval

<b>Approved on:</b>	
<b>By:</b>	 General Manager, Investigations and Enforcement Branch
<b>Signature:</b>	
<b>Period of effect:</b>	
<b>Review date:</b>	

## Version control

Version	Date	Author	Approver
0.1	27/06/2013		
0.2	28/06/2013	 review and minor changes.	

0.3	19/07/2013	██████████ – Legal Services comments	██████████
0.4	19/07/2013	██████████ – Acceptance of legal services comments	██████████
0.5	30/07/2013	██████████ – Review following CEO comments	██████████
0.6	02/09/2013	██████████ – Changes to CER authorised officers	██████████
1.0	16/09/2013	██████████ – Approved.	██████████
1.1	11/08/2014	██████████ – Update following nomination of authorised officers and passage of Public Governance, Performance and Accountability Act 2013	██████████
2.0		██████████	██████████ – Approved.



# Appendix A: Enforcement agency – Authorisation and notification for access to existing information or documents

*Telecommunications (Interception and Access) Act 1979 (Cth)*

## 1 Authorised officer

- (1) The Clean Energy Regulator is an enforcement agency within the definition of 'enforcement agency' in subsection 5(1) of the *Telecommunications (Interception and Access) Act 1979* (the Act).
- (2) I, [NAME], [^POSITION/POSITION NUMBER/RANK], am an authorised officer of Clean Energy Regulator within the definition of 'authorised officer' in subsection 5(1) of the Act as I am
  - ☐ the head of the Clean Energy Regulator or a person acting as that head
  - ☐ the deputy head of the Clean Energy Regulator or a person acting as that deputy head
  - ☐ a person who holds, or is acting in, an office or position in the Clean Energy Regulator covered by an authorisation of the head of Clean Energy Regulator under subsection 5AB(1) of the Act.

## 2 Authorisation

- (1) Acting under subsection 179(2) of the Act, I authorise the disclosure of the following specified information or documents, being information or documents that came into existence before the time the person from whom the disclosure is sought, being [person/company from whom the disclosure is sought], receives notification of the authorisation:

[short particulars of the information and/or documents sought to be disclosed]

- (2) I am satisfied that the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty.

## 3 Notification and disclosure

Acting under subsection 184(3) of the Act, I notify the person listed above of this authorisation.

The information or documents authorised to be disclosed by this authorisation should be delivered to **Error! Reference source not found.** by the following means:

[particulars of the facsimile number, electronic address or other electronic means by which the information should be provided to the agency]

Dated

.....

Authorised officer

\* Omit if not applicable

^ Use same descriptor as used in instrument approving person as an authorised officer

## Appendix B: List of authorized officers

The following list of management positions in the CER have been authorised by the Chair and Chief Executive Officer as “authorised officers” under the *Telecommunications (Interception and Access) Act 1979* (Cth).

Only these officers are able to authorise the disclosure of telecommunications data in accordance with these Standard Operating Procedures.

### Schedule

---

Chair and Chief Executive Officer, Clean Energy Regulator

Executive General Manager, Reporting and Carbon Market Division

General Manager, Investigation and Enforcement Branch