Auditor-General for Australia

Australian National Audit Office

10 February 2022

Ms Lucy Wicks MP
Chair
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

By email: jcpaa@aph.gov.au

Dear Ms Wicks

Review of the *Auditor-General Act 1997* – additional ANAO submission

I am writing to provide an additional submission to the Joint Committee of Public Accounts and Audit's (JCPAA's) inquiry into the *Auditor-General Act 1997* (the Act). This additional submission relates to the Auditor-General's information gathering powers under the Act.

The ANAO's original submission of 27 November 2020 (submission 2 to the inquiry) observed at paragraph 50 that in relation to the Auditor-General's information gathering powers, the ANAO had not encountered any major practical issues and did not consider that any changes were required to Division 1 of Part 5 of the Act. That part of the Act includes sections 32 and 33, which set out the information gathering powers.

The efficient collection of sufficient and appropriate information, to form the evidence base to support audit opinions and conclusions, is a key issue in the ANAO's role in supporting the Parliament through independent reporting. Throughout the inquiry, the JCPAA has shown an interest in the collection of evidence in the ANAO's work with the emergence of new technology. As you know, the Act came into effect at a time when information collection was largely paper-based. The ANAO has recently received legal advice that raises questions about the operation of sections 32 and 33 in relation to the Auditor-General's ability to: require remote access to entity ICT systems for evidence gathering purposes; and to specify the form in which requested information is provided by entities. This submission is to bring to your attention the potential for legislative amendment to modernise and clarify the exercise of information-gathering powers with respect to how information is collected.

The legal advice was sought after issues relating to remote access were raised by an audited entity in late 2021. A copy of the legal advice obtained by the ANAO is at Attachment A.

By way of background, generally the ANAO accesses information held by an audited entity with the cooperation of the relevant entity. The Auditor-General only uses the powers in sections 32 and 33 of the Act in rare circumstances, such as where an entity requests they be used to avoid doubt or provide comfort, or where it is needed to enable the ANAO to obtain oral evidence.

GPO Box 707, Canberra ACT 2601
38 Sydney Avenue, Forrest ACT 2603
Phone: +61 2 6203 7300
Email: grant.hehir@anao.gov.au

Given the level of technological advancement in recent years, the ANAO now regularly accesses information from audited entities by remote means, while not physically on entity premises, with the entity's cooperation. This can involve a range of access arrangements, including remote login to entity systems (accessed from the ANAO staff member's work computer) and/or the provision of tools to relevant ANAO staff (such as network cabling to ANAO office premises and the provision of entity laptops to enable remote access). Remote access arrangements have supported the efficient and effective conduct of ANAO audits and have reduced the impact of audit processes on staff in audited entities, while also enabling audit work to continue during periods where entity premises cannot be accessed (for example, during COVID-19 lockdowns) or when it is not practical to travel to entities for audit work (for example, due to travel restrictions for entities not located in Canberra). This remote access approach has been adopted across all audit and assurance functions conducted under the Act and includes remote ANAO access to classified entity systems.

In summary, the legal advice indicates that the text of section 33 of the Act does not support remote access, as it is drafted to apply subsequent to an authorised ANAO official physically entering and remaining on an entity's premises.

In contrast, section 32 of the Act is a broad information-gathering power available to the Auditor-General and includes a power to direct a person to produce any documents in their custody or control. Databases held by agencies that are the subject of an audit will generally consist of 'documents' in this sense, and it would be reasonable to proceed on the basis that making data available remotely in a manner agreed with the Auditor-General could be regarded as 'producing' those documents.

The advice further indicates that if the agency holding the data objects to making the database available remotely, it could insist on complying with any demand for production by producing the data in another way, for example by giving a printed copy of it to the Auditor-General. That is because section 32 creates an obligation on a person receiving a notice to produce the documents specified in the notice. It does not give the Auditor-General a general power to specify the form in which a document is produced. The ANAO acknowledges that this might be a rare circumstance but the form of production can affect the ANAO's ability to efficiently and effectively review and analyse the material.

The legal advice suggests that consideration could be given to seeking an amendment to the Act which would update these powers to allow more clearly for remote access and to enable the Auditor-General to specify the form of production. It is not intended that any amendment increases the information-gathering powers in respect of the type of information that can be sought, just the form and/or manner in which information is provided.

In the circumstances, the Committee may wish to consider the benefit of amending sections 32 and 33 of the Act to address the issues raised in the legal advice and provide clarity for future ANAO information-gathering purposes. There are a range of options that could be considered for this purpose and the attached legal advice provides some initial thinking on options.

I would be happy to further discuss this matter with the Committee to inform its inquiry.

Yours sincerely

[redacted]

Grant Hehir
Auditor-General

Attachment A

OFFICIAL: SENSITIVE
Legal-Privilege

Prepared for Australian National Audit Office
Ms Carla Jago
Group Executive Director
Performance Audit Services Group
Our ref: 21009302
7 February 2022

Exercising information access powers remotely

1. Our advice is sought about the application of the ANAO's information gathering and access powers by remote means, for example where an agency cooperatively provides access to its computer systems. Your question, our answer and the reasons for our answer are set out below.

Summary

Q1

Do the information gathering and access powers in Part 5 of the *Auditor-General Act 1997* (the Act), including section 33, support the ANAO accessing information from audited entities 'remotely' for the conduct of Auditor-General functions in Part 4 of the Act (noting that a number of limitations regarding the use of sections 32 and 33 are specified in section 31 of the Act)?

2. The information-gathering power in s 32 of the Act offers the stronger means for obtaining access to data remotely. It is doubtful that s 33 of the Act supports access of this nature in its current terms.

3. Consideration could be given to seeking an amendment to the Act which would update these powers to allow more clearly for remote access, if that is consistent with the policy intention. The Joint Committee of Public Accounts and Audit (JCPAA) is currently inquiring into the Act, including the Auditor-General's information gathering powers, and this inquiry might offer a timely opportunity to raise any identified deficiencies in the existing powers.

Reasons

The s 33 power is probably only engaged when authorised officials are on the premises

4. Sections 32 and 33 are set out below, for reference. We understand that s 33 would be the preferred means of accessing data remotely. For the reasons which follow, in the event of a challenge we consider it doubtful that s 33 would be found by a court to be able to be used in that way.

The text of s 33 supports powers being conditioned on officials being on relevant premises

5. The text of s 33 does not support remote access. In general terms, s 33(1)(a) relevantly permits entry to particular types of premises. Section 33(1)(b) permits access to documents or other property, and s 33(1)(c) permits examination and copying of documents. The difficulty is that ss 33(1)(b) and (c) are drafted to apply subsequent to an authorised official entering and remaining in premises under s 33(1)(a). Those paragraphs cannot be read in isolation. To attempt to do so would result in each of them comprising an ambiguously broad power of uncertain scope, along the lines that the Auditor-General or an authorised official is entitled to full and free access at all reasonable times to any documents or other property, with no clear connection to the various Commonwealth related entities or premises in respect of which the s 33(1)(a) power is enlivened.

6. This conclusion is consistent with other aspects of s 33. In particular, s 33(2) requires authorised officials to produce written authority to exercise powers under Div 1 of Part 5 of the Act, upon request from an occupier, *in order to enter or remain on premises*. There is no mention of requiring evidence of authority to do anything from outside the relevant premises. It seems unlikely, in our view, that Parliament would have intended authorised officials to be able to exercise access powers remotely, without making some sort of equivalent provision for them to produce proof of authority.

7. There is nothing in the Explanatory Memorandum accompanying the Auditor-General Bill 1996 which supports a contrary interpretation. If anything, it seems to have been anticipated that these powers will be exercised on site by authorised officials.

Contrary arguments could be made, but they do not necessarily overcome the terms of s 33

8. While there is much to be said from a practical perspective about the merits of authorised officials being empowered to access data remotely, especially given the increased reliance on electronic transactions since the powers were enacted, we have not identified a compelling basis for implying that power in s 33. To find such an implication, it would be necessary to establish with some certainty that, despite the terms of s 33, Parliament did not intend that authorised officials needed to be physically present to exercise the powers.

9. It might be argued, for example, that the fundamental purpose of the power is to facilitate access to documents and that there is nothing to be gained in insisting that an authorised official attend premises to access documents on the property when they are held in a computer system or on a server or in cloud facilities. That is especially so when an inspection can be accomplished less intrusively if done remotely.

10. It might also be argued that it was not intended that the powers in the Act be more limited than those in its predecessor, the *Audit Act 1901* (the Audit Act). Section 48E of that Act is set out below, for comparison. It included similar powers for an 'authorized person' in the course of conducting an efficiency audit, but the equivalent aspect of s 48E was not drafted such that it was only engaged when the authorized person was on the premises. Instead, s 48E(3) gave a clear power for the authorized person to, 'at all reasonable times, have full and free access to all records in the possession of' certain persons and bodies. It was then followed by s 48E(4), which gave a separate entry and inspection power. At face value, it appears that s 48E(3) would have been able to be applied in a remote access situation, in contrast to s 33 of the Act which lacks that flexibility because it contemplates the 'access to documents' power being engaged only upon entry to relevant premises.

11. The difficulty with relying on these arguments in support of interpreting s 33 to permit remote access is that they would need to overcome the fact that they are at odds with its specific terms. At face value, s 33 appears to contemplate that authorised officials will exercise the powers on the premises of the relevant entity. While it is open in some situations for the meaning of a statute to be modified by implication, a court might consider that the need to do so in this case exists only to address a gap in the legislation. It might conclude that Parliament enacted the power in these terms 25 years ago because at that stage inspections took place on the other agency's premises as a matter of course, and remote access was not envisaged. We understand from your instructions, set out below, that the remote access practice developed given 'the level of technological advancement in recent years'. If so, this would not provide a strong basis for interpreting the power more broadly than its terms. As Kiefel CJ, Gageler and Nettle JJ observed:

> The task of construction of a statute is of the words which the legislature has enacted. Any modified meaning must be consistent with the words in fact used by the legislature. Words may be implied to explain the meaning of the text. The constructional task remains throughout to expound the meaning of the statutory text, **not to remedy gaps disclosed in it** or repair it. [1]
>
> (footnotes omitted, emphasis added)

12. It is also worth noting that coercive powers tend to be construed strictly in the event of an ambiguity,[2] although the weight of that principle in relation to a power like this - which is applied only to entities with a connection to Commonwealth activities - might be open to argument.

---

1 *HFM043 v Republic of Nauru* (2018) 359 ALR 176, [24].

2 See eg *George v Rockett* (1990) 170 CLR 104, 110-11.

13. We have considered whether there are any other Commonwealth laws which would assist to support a contrary conclusion, including the *Electronic Transactions Act 1999* (the ET Act), but we have not identified any provisions which will do so. On balance, we do not consider that you can proceed confidently on the basis that s 33 of the Act would be found by a court to apply to and support remote access.

The power in s 32 is probably available in these circumstances

14. In contrast, s 32 of the Act is a broad information-gathering power available to the Auditor-General. In principle, it could be delegated under s 29 of the Act. It includes a power to direct a person to produce any documents in their custody or control.

15. Databases held by agencies that are subject of an audit will generally consist of 'documents' in this sense.[3] In our view, it would be reasonable to proceed on the basis that making data available remotely in a manner agreed with the Auditor-General could be regarded as 'producing' those documents.

Providing means of access to data is arguably a form of 'production'

16. Noting the audit and review functions of the Auditor-General, if the Auditor-General considered that access to an entire database was warranted then it would seem open to issue a notice to a person within an agency being audited, requiring 'production' of the database. The notice would generally need to be addressed to a 'person', such as the agency head or chief information officer, at least in respect of non-corporate entities.

17. Provided that the parties agreed to facilitating an inspection of data remotely in this way, we consider that it would be reasonable to proceed on the basis that the production obligation can be discharged by making the database available electronically. The word 'produce' will be interpreted in the context of the statute in which it appears,[4] and the purpose that is evident in the terms of s 32 is broad, aimed at enabling the Auditor-General to obtain any information and other material that is required for certain functions. There appears to be no reason to insist on a narrow or unduly confined interpretation. Helpfully, in this respect, noting that the agency being audited will retain possession of the database, 'produce' has been held not to require that possession be parted with.[5]

18. The ordinary meaning of 'produce' will be the starting point. The *Macquarie Dictionary Online* definitions relevantly include 'to yield, provide, furnish or supply'. The *Oxford English Dictionary* offers a more expansive definition, relevantly including 'to present to view or notice; to show or provide (something) for consideration, inspection or use'.

19. Given that the documents exist in digital form, if a representative of the body being audited authorised the Auditor-General to access its data, and gave the Auditor-General the means to do so, then in our view it would be open to consider that the

---

3 See the definition of 'document' in s 2B of the *Acts Interpretation Act 1901*(the AI Act), meaning 'any record of information'. A 'record' is defined in s 2B of the AI Act as including information stored or recorded by means of a computer.

4 *Hanfstaengl v American Tobacco Co* [1985] 1 QB 345, 355.

5 *Button v Evans (No 2)* (1984) 75 FLR 252, 259.

data has been 'produced' to the Auditor General in this sense. By equipping the Auditor-General with the means to access the data, it will effectively have been provided for inspection, consistently with the *Oxford* definition. This interpretation might be thought to have added weight in cases where cabling and other equipment is given to the Auditor-General as a vehicle for accessing the data, although in our view it remains open even where the access is facilitated through less direct means.

20. However, if the agency holding the data objects to making the database available remotely in this way, then in our view it could insist on complying with any demand for production by producing the data in another way, for example by giving a copy of it to the Auditor-General. That is because s 32 creates an obligation on a person receiving a notice to produce the documents specified in the notice. It does not give the Auditor-General a general power to dictate the form in which a document is produced. If a notice specifies a document or set of documents in general terms, then in principle the person receiving the notice would comply if they produced the specified document/s in any readable form. [6] Of course, it might be anticipated that in the ordinary course of events a notice recipient would be prepared to cooperate with reasonable requests from the Auditor-General as to the form in which a document is produced.

21. That said, if the notice recipient is not prepared to cooperate in this way, and if it is necessary to access a document in electronic form, for example because metadata or some other information required by the Auditor-General will only be available electronically, then it should be possible to specify in a notice a particular version of that document for production. So, for example, rather than issuing a notice describing a file in general terms, and then separately purporting to insist that it be provided electronically, it may be possible for the notice to specify a particular version of a file, including all metadata associated with its creation and use.

22. Arguments might be put that s 32 would not apply to remote access, for example because this proposal involves 'making the data available', rather than 'producing' it in a conventional sense. In this context our interpretation is not beyond dispute. However, we consider that it is open and appropriate in the context of the objects of the Act. In any event, in our view s 32 offers a stronger legal basis to pursue this solution than relying on s 33.

23. We considered briefly an alternative argument that s 32(1)(a) might apply here and that remote access involves the 'providing' of 'information'. The difficulty is that there is a prospect that 'information' in this sense is liable to be interpreted to mean 'knowledge' rather than documents in electronic form. While that argument could be advanced in the alternative, we doubt that it would be stronger than relying on s 32(1)(c).

---

6 There is generally an obligation to produce computer records in a form that is capable of being understood by the person requiring production, unless the person requiring production permits otherwise: see AI Act, s 25A. For completeness, because the database presumably contains documents which exist in digital form, and not in the form of 'paper, an article or other material', we do not consider that s 11(1) of the ET Act is applicable here.

Sections 32 and 33 are not available for certain purposes

24. As noted in your Question, the exercise of these powers is subject to s 31 of the Act, which sets out certain situations in which neither ss 32 nor 33 can be used. It follows that this option will only be available for the purpose of, or in connection with, the Auditor-General functions that are not specified in s 31.

The JPCAA is currently inquiring into relevant powers

25. In researching the legislative history of the Auditor-General's powers we noticed that the JCPAA is currently inquiring into the Act, and that the terms of reference expressly include the Auditor-General's information gathering powers. This may present a timely opportunity to seek the JCPAA's support for modernised powers in this respect.

26. The form that any updated powers might take will be a matter for policy judgment, and for discussion with the Department of the Prime Minister and Cabinet as the Department responsible for administering the Act. It would be open to consider a range of options, depending upon operational requirements and any broader issues that may be identified.

27. If it was simply sought to make a relatively confined amendment to the existing powers, then it would be possible to consider adding to s 33 a power which is separate from that currently in s 33(1), and which is not conditioned on there being an entry to premises. Careful attention would need to be given to its scope, and to whether input from different stakeholders needs to be taken into account, for example in the event that there are particular security or other sensitivities in the types of access which may be given to particular databases.

28. The placement and the terms of any amended power within s 33 should be discussed with the Office of Parliamentary Counsel. Subject to stakeholder input, it might, for example, provide to the effect that the Auditor-General or an authorised official is entitled at all times to access and copy any documents, records or databases held by the Commonwealth, a corporate Commonwealth entity, a Commonwealth company or a Commonwealth partner. It could state expressly that the Auditor-General or an authorised official may require that access be provided electronically where the documents or records exist in electronic form, including by requiring remote access to databases or other records, where remote access can reasonably be achieved consistently with applicable security requirements.

29. If an approach along these lines is adopted, consideration should be given to whether s 33(2) would be amended to require proof of authority for access of this nature. Consideration might also be required as to whether or not it would be appropriate to extend the existing offence in s 33(3), relating to the failure to provide reasonable facilities for the effective exercise of powers, to apply to any amended power. Again, that will be a matter for policy judgment. If the offence is extended, then it will need to identify the persons responsible for facilitating access, and who would potentially be liable in the event of non-compliance. Alternatively, consideration could be given to whether it is necessary to retain the existing offence in its current form.

Context

Background

30. A summary of the background we have been provided is as follows.

31. Generally, the ANAO accesses information held by an audited entity with the cooperation of the relevant entity. The Auditor-General only uses the powers in s 32 of the Act in rare circumstances, such as where an entity requests they be used to avoid doubt or provide comfort, or where it is needed to enable the ANAO to obtain oral evidence.

32. Given the level of technological advancement in recent years, the ANAO now regularly accesses information from audited entities by remote means, while not physically on entity premises, with their cooperation. This can involve a range of access arrangements, including remote login to entity systems (accessed from the ANAO staff member's work computer) and/or the provision of tools to relevant ANAO staff (such as network cabling to ANAO office premises, the provision of entity laptops to enable remote access, etc). Remote access arrangements have supported the efficient and effective conduct of ANAO audits and reduced the impact of audit processes on staff in audited entities, while also enabling audit work to continue during periods where entity premises cannot be accessed (e.g. during COVID-19 lockdowns) or when it is not practical to travel to entities for audit work (e.g. due to travel restrictions for entities not located in Canberra). This remote access approach has been adopted across all audit and assurance functions conducted under the Act, and includes remote ANAO access to classified entity systems.

33. An audited entity has raised that in the absence of entity cooperation, s 33 of the Act may limit the ANAO's ability to access information remotely due to the definition of 'premises' in s 33(4) — which states that 'premises' includes any land or place'. That is to say, if the Auditor-General is obliged to 'invoke' his powers under Part 5 of the Act (which includes ss 32 and 33) to access information, the information held by the relevant entity cannot be accessed remotely by the ANAO.

34. You note that in many cases, entity records are no longer physically 'present' on entity premises, but are accessed 'remotely' by entities themselves from data servers and 'cloud' facilities located elsewhere.

Legislation

35. Sections 32 and 33 of the Act are in the following terms:

32 Power of Auditor-General to obtain information

(1) The Auditor-General may, by written notice, direct a person to do all or any of the following:

(a) to provide the Auditor-General with any information that the Auditor-General requires;

(b) to attend and give evidence before the Auditor-General or an authorised official;

(c) to produce to the Auditor-General any documents in the custody or under the control of the person.

Note: A proceeding under paragraph (1)(b) is a "judicial proceeding" for the purposes of Part III of the *Crimes Act 1914*. The Crimes Act prohibits certain conduct in relation to judicial proceedings.

(2) The Auditor-General may direct that:

(a) the information or answers to questions be given either orally or in writing (as the Auditor-General requires);

(b) the information or answers to questions be verified or given on oath or affirmation.

The oath or affirmation is an oath or affirmation that the information or evidence the person will give will be true, and may be administered by the Auditor-General or by an authorised official.

(3) A person must comply with a direction under this section.

Penalty: 30 penalty units.

Note 1: Chapter 2 of the *Criminal Code* sets out the general principles of criminal responsibility.

Note 2: Section 4AA of the *Crimes Act 1914* sets the current value of a penalty unit.

(4) The regulations may prescribe scales of expenses to be allowed to persons who are required to attend under this section.

(5) In this section:

authorised official means an official of a non-corporate Commonwealth entity who is authorised by the Auditor-General, in writing, to exercise powers or perform functions under this section.

33 Access to premises etc.

(1) The Auditor-General or an authorised official:

(a) may, at all reasonable times, enter and remain on any premises occupied by the Commonwealth, a corporate Commonwealth entity, a Commonwealth company or a Commonwealth partner; and

(b) is entitled to full and free access at all reasonable times to any documents or other property; and

(c) may examine, make copies of or take extracts from any document.

Note: Paragraph (1)(a) does not expressly refer to non-corporate Commonwealth entities because these entities are legally part of the Commonwealth.

(2) An authorised official is not entitled to enter or remain on premises if he or she fails to produce a written authority on being asked by the occupier to produce proof of his or her authority. For this purpose, ***written authority*** means an authority signed by the Auditor-General that states that the official is authorised to exercise powers under this Division.

(3) If an authorised official enters, or proposes to enter, premises under this section, the occupier must provide the official with all reasonable facilities for the effective exercise of powers under this section.

Penalty: 10 penalty units.

Note 1: Chapter 2 of the *Criminal Code* sets out the general principles of criminal responsibility.

Note 2: Section 4AA of the *Crimes Act 1914* sets the current value of a penalty unit.

Note 3: Section 149.1 of the *Criminal Code* deals with obstruction of Commonwealth public officials.

(4) In this section:

authorised official means an official of a non-corporate Commonwealth entity who is authorised by the Auditor-General, in writing, to exercise powers or perform functions under this section.

premises includes any land or place.

36. As discussed above, the equivalent powers in the now-repealed Audit Act were cast in broader terms which were more adaptable to developments of this nature. Section 48E of that Act provided as follows:

48E Investigations and access to premises and records

(1) An efficiency audit of operations of a relevant body shall be conducted by the Auditor-General, subject to this Act, in such manner as the Auditor-General thinks fit.

(2) Without limiting the generality of subsection (1):

(a) an efficiency audit of operations of a relevant body may be carried out in conjunction with, and as part of, an inspection and audit of the accounts of the body that is being carried out by the Auditor-General under this Act or under another Act; and

(b) any information obtained by the Auditor-General, in the course of carrying out an inspection and audit of the accounts of a relevant body, whether as a result of inspecting the accounts or records of the body or otherwise, may, whether or not the Auditor-General was at the same time carrying out an efficiency audit of operations of that body, be treated as having been obtained for the purposes of carrying out such an audit.

(3) Without prejudice to the powers conferred on the Auditor-General by any other provision of this Act, the Auditor-General or an authorized person shall, at all reasonable times, have full and free access to all records in the possession of:

(a) a relevant body;

(b) a person employed by, or under the control of, a relevant body;

(c) a person employed as a member of a Commonwealth organization; or

(d) any other person;

being records relating, directly or indirectly, to operations that have been, or are being, carried on by a relevant body or to procedures that have been, or that are being, followed by a relevant body for reviewing any such operations, and may make a copy of, or take extracts from, any such records.

(4) For the purposes of an efficiency audit of operations of a relevant body that is being carried out under this Act:

(a) the Auditor-General, or an authorized person, may, at any reasonable time, enter any place occupied by the body and carry out an examination of the operations of the body at the place; and

(b) the Auditor-General, or an authorized person, is entitled to inspect, at a reasonable time arranged with the principal officer of the body, any records relating to the operations of the body that are kept at premises entered by him under this section, and to take copies of, or extracts from, any such records.

(5) Nothing in this section shall be taken to restrict the operation of any other section of this Act in relation to efficiency audits of operations of a relevant body.

Contact

37. Tara McNeilly, Senior General Counsel, has read and agrees with this advice. Please let us know if you would like to discuss any aspect of it.

[redacted]

Paul Marshall
Senior General Counsel
[redacted]