PUBLIC ACCOUNTS AND ESTIMATES COMMITTEE

Inquiry into Fraud and Corruption Control in Local Government: a Follow-Up of Two Auditor-General Reports

Melbourne – Monday 28 July 2025

MEMBERS

Sarah Connolly – Chair
Nicholas McGowan – Deputy Chair
Jade Benham
Michael Galea
Mathew Hilakari
Lauren Kathage
Aiv Puglielli
Meng Heang Tak
Richard Welch

WITNESS

Sean Morrison, Victorian Information Commissioner, Office of the Victorian Information Commissioner.

The CHAIR: I declare open this hearing of the Public Accounts and Estimates Committee, and I ask that mobile telephones please be turned to silent.

On behalf of the Parliament, the committee is conducting this inquiry into fraud and corruption controls in local government. I advise that all evidence taken by the committee is protected by parliamentary privilege. However, comments repeated outside of this hearing may not be protected by this privilege.

Witnesses will be provided with a proof version of the transcript to check, and verified transcripts, presentations and handouts will be placed on the committee's website.

I welcome Sean Morrison, the Victorian Information Commissioner. You are very much welcome here this afternoon.

Mr Morrison has provided a written statement to the committee in lieu of an opening statement this afternoon. Therefore, we will proceed directly to questions from members, and we will start with Ms Benham.

Jade BENHAM: Thank you for joining us and being our last witness this afternoon. In your statement or submission, it was noted that it is unreasonable that local councils are excluded from part 4 of the *Privacy and Data Protection Act*. What are the consequences then of excluding local councils from the Act, and how is it increasing the risk of fraud and corruption? We have heard today from a number of councils concerned about this and cybersecurity in general. So can you run us through what the consequences are?

Sean MORRISON: To put it simply, the consequences are that they are off our radar and not under our remit. I will pick through that. Part 4 applies what is effectively an information security overlay, and that is each organisation that is subject to part 4 is required to do a SRPA – a security risk profile assessment. It is like a gaps analysis of noting where your security risks are across the organisation. Then they are also required to submit a protective data security plan every two years, and we get that and assess that. Those plans have 12 standards in them and 98 elements. How that equates to fraud and corruption controls is those standards cover things like: everyone in the organisation is aware of their security obligations, there are proper offboarding and onboarding protocols and there are things like appropriate access controls. So it provides a framework that is in line with current standards that councils need to comply with. You will note that we say we need mandatory reporting, but there is a reporting element there as well.

Jade BENHAM: In terms of legislative reform, then, obviously legislative reform is going to be necessary, so how is that then going to be implemented? We have heard, again, councils today say that systems can be different council to council, so how do we implement this and how do we legislate for it?

Sean MORRISON: How we legislate is quite simple: we make councils subject to it, so we remove them from the exclusionary provision. I will leave that to the drafters. On how we implement it, it is still a risk-based framework, so it is not 'You must have system X', it is 'You must have a certain type of control. How you implement the control is up to you.' So it accounts for different systems. The other thing that should be noted is that councils, by way of some peculiarities of the legislation, are already doing some of this reporting, so they are aware of the framework. I have listened to a lot of the witnesses talk about the impost on resources. Most of them understand the framework. They engage with us through our education activities and resources. I think it is a matter of making sure that everyone is in – the rising tide lifts all boats, so there might be some stragglers, so it creates that corpus of knowledge as well. Legislation to me is easy, and it can be legislation that is deferred – you know it is coming – and then on the implementation part I think they are part way there.

Jade BENHAM: Why on earth were councils excluded from part 4 in the first place, in your opinion?

Sean MORRISON: One, we do not know, but it could have been at the time that councils did not have the range of information that they have now. We know that they are hooked into a lot of the Victorian public sector's information schemes, from maternal and child health and Child Link. So it could have been with the value of the information they had back then it was much less desirable for bad faith actors. It could even have been a resource challenge. It could be any of those.

Jade BENHAM: Thank you. I will hand over to Mr Welch to finish our time.

Richard WELCH: Thank you. In regard to cybersecurity, the impression I got from most of the councils that we have spoken to is they are chasing their tails on this, the difference between best practice and worst practice is very, very wide indeed and it is an arms war against those who would use it against us. In your view, what is the scale or the status of the risk we are now exposed to? If it was a traffic light system or out of a scale of 10, are we currently in very treacherous waters or are we actually catching up and getting on top of it?

Sean MORRISON: We do not have exact oversight of local government, so I will just caveat with that. We get some protective security data plans, but we do not know whether they cover all of their information or just the committees of management – smaller things. I would say we are at amber, and the attestations we are getting show an average compliance with what we require. I think what we have been saying at OVIC for a while is that you need to treat it like not if you will have an incident but when you will, and these controls help mitigate that risk, that loss, and also help the clean-up afterwards. I think everyone should be in the alert but not alarmed sort of phase.

Richard WELCH: You might not have visibility of this, but where do you think our councils are in terms of readiness for that mitigation?

Sean MORRISON: I really would not want to answer that except to say that they would be more ready if they were subject to part 4.

Richard WELCH: Fair call. Thank you, Chair.

The CHAIR: Thank you. We will go to Ms Benham.

Jade BENHAM: I will keep going, if that is okay. With regard to the data that is held by councils – and we have already said that they are excluded and that OVIC does not have oversight over it – should councils be sharing fraud and corruption data with one another more freely? Is that again going to be an issue with that information-sharing framework? How could it be done to facilitate best practice across councils, especially those that do not have the resources that they require?

Sean MORRISON: We have seen in our own experience – our information security unit provides VISN, which is really an insights network, which talks about those fraud and corruption risks across the whole public sector. We think there is value there. If it was the same framework for councils, I think that would be helpful because you can learn from others' mistakes or near misses. If it is just public sector data and it is not personal information and identifiable, on the face of it – apart from if there are secrecy provisions that apply or, for example, if those things have been referred to IBAC or somewhere else where you have to tread carefully – I do not see why raw statistical data could not be shared or there would be a prohibition on that. You will note we have asked for a mandatory reporting framework. Some people might be scared or hesitant to share that because it exposes them to corporate or reputational risk. But our view is it is better to have it out in the open because sunlight is the best disinfectant – it really helps. We need to move past that 'Let's bring it internally and deal with it' and think about it like everyone is being exposed to these security risks.

Jade BENHAM: You can understand why organisations may be hesitant to share information given the risks involved with that. How do they go about mitigating that and being able to share information among one another?

Sean MORRISON: Well, it could be through confidential networks and a framework of what is shared in the first instance – so it is high level – and then the framework comes down to something more granular. The chief information officers or chief data officer or anyone who has got responsibility for that then digs in deeper. I totally understand you do not want to be exposing warts and all to threat actors, but there definitely is value in allowing your incident regime to be exposed to others.

Jade BENHAM: In those smaller councils, though, which may not have chief information officers or may have a department of two people that oversee a huge amount, the framework would obviously need a certain amount of flexibility to be able to cater to those smaller councils.

Sean MORRISON: Definitely. A good framework should fit all. I have not listened to all witnesses, but I heard today about potentially sharing resources and also integrity bodies putting out packages and things like that. I think in the smaller councils definitely the reason is you may not have the resources, but it is not an excuse, so you have to lean in. Also, the bigger councils should take it as I think a recognition of their expertise that they can assist others.

Jade BENHAM: Good point. Lastly, in your opinion again, what is the minimum level of cybersecurity training that council staff and councillors all should be receiving?

Sean MORRISON: The minimum level is some training – I know that is not really answering the question – training that is tailored to their organisations' risks. I think that apart from a lexicon, like a data dictionary, and some things like email phishing and all of those basics, which are quite basic across all sectors, the training they should receive is on the risks specific to their organisation. If there are, for example, interactions with transactions, money, corporate functions, procurement, the training would be specific to those risks, I think, because information security is not just a one and done; it presents different challenges for each individual in the organisation.

Jade BENHAM: Would it make each organisation more accountable for having identified where their biggest risk profiles are?

Sean MORRISON: That is what the SRPA does if you are under part 4. Your training and your education must meet those requirements for your organisation, individualised. We are back to everyone in part 4.

Jade BENHAM: Yes. Great. Thank you.

Richard WELCH: I have got one more if I have got time.

The CHAIR: Great. Back to Mr Welch.

Richard WELCH: In regard to KYC protocols around grants, do you have any evidence or sentiment around why that would be necessary at a grassroots local government level? And are there things that are being missed by the council's existing protocols that KYC would capture?

Sean MORRISON: I will have to show my ignorance – KYC?

Richard WELCH: Know your customer.

Sean MORRISON: Oh, sorry. Okay. Forgive me. Look, I am not aware of that particular protocol, know your customer. If you are able to elaborate on it I can expand further.

Richard WELCH: No. Okay. Thank you.

Sean MORRISON: Thank you.

Richard WELCH: Thank you, Chair.

The CHAIR: Thank you, Mr Welch. Ms Kathage.

Lauren KATHAGE: Thank you, Chair. Thank you very much for being here. I just wanted to ask a little bit more about council not being included in the same provisions, and the difference between VPS agencies and councils then holding the same information, making council more of an attractive target for people who would seek to breach cybersecurity or things like that. Can you speak a bit to what other difficulties it poses, having different rules between VPS agencies and councils?

Sean MORRISON: Well, apart from the threats you have identified – that your security environment is only as strong as the weakest link – I think it creates confusion for agencies, it creates confusion for information security practitioners and it creates different playing fields and different standards. And there may even be market forces that could provide better value for money if everyone was subject to the same information security framework as well, because you might get that buying power. But at the moment there is a disconnect

and it just does not help. Confusion is the main thing, and once you have confusion you do not have adherence and then you have security risks.

Lauren KATHAGE: Is it correct that libraries and hospitals are treated the same as council?

Sean MORRISON: I will have to come back on libraries, but hospitals are exempt from part 4 as well and so are universities.

Lauren KATHAGE: Thank you. Recent history would give us pause around the use of electronic information to detect fraud, following the robodebt inquiry. In terms of the connection between different data holders, what do you see as being necessary safeguards for the rights and wellbeing of people that might be subject to the cross-referencing of data?

Sean MORRISON: Well, if it is just data, I think the main worry is that when you get those datasets meshed with each other it becomes identifiable information. So it is not just used for statistical analysis and planning – then you are drilling down to an individual. And if you are sharing personal information, there are requirements. You cannot just be providing personal information to another organisation just because it is convenient; it needs to be in line with the reason you collected it. So there are controls there. I will say that now AI is in everything, there are also other issues with AI running over these datasets, which might be used to find fraud and corruption, and OVIC has published resources on that. The concern is if you are using a publicly available tool you do not control that information, you do not know where it is going and you do not know where it is stored. So there are a number of issues. We recognise that audit is an important tool, but it needs to comply with privacy practices and also AI guidance.

Lauren KATHAGE: Thank you for that. With the risk around the weakest link – which you have identified councillors being in some circumstances – besides not being excluded in the relevant provision, what other ways do you think that that risk can be mitigated?

Sean MORRISON: Councils do look at our resources and attend our training events. I just want to clarify that I hope councils do not think I am tarring them with the weakest link brush, but it is just an example. I think education is definitely the way out, because if you can train your staff – and that is not just in privacy and information security, that is around reporting corruption and fraud – and also have a strong audit program, I think they are the ways that corruption can be dealt with, especially with the governance around local councils.

Lauren KATHAGE: If you had a magic wand and you could provide all of the support and information to councils that you wanted, what would that look like?

Sean MORRISON: I will say – and I brought them along and I am happy to provide them to the committee later on – we have done three specific resources for councils about releasing information, about privacy considerations and around the Victorian Protective Data Security Standards. It would be great to potentially do roadshows with integrity agencies to get out to meet councils and also to have a bespoke training program that we could assist with and a helpline, but I do not have a magic wand.

Lauren KATHAGE: In your submission you mentioned the integrity agencies. In your submission you wrote about a possible role or greater collaboration between yourselves and other integrity agencies. What do you see as being the main benefit there in terms of fraud and corruption control, and are you able to self-identify some risks with that as well?

Sean MORRISON: We are developing our new regulatory action plan, which will have greater stakeholder engagement, and reaching out across the integrity framework to make sure that if there is a risk there – 'Does it cross over our jurisdiction?' The benefit definitely is for us to be more proactive than reactive but also to potentially add to a resource that someone is drafting. There are risks where information cannot be shared, and one of the risks might be that, due to the secrecy provisions in our various legislations, it is really consultation only with no benefit. I think the risk is that when you have those interactions with other agencies you have to be thinking with the end user in mind, not just of a tick-the-box exercise. We will definitely be going through that, especially around the Local Government Inspectorate. I heard today some things about the Local Government Inspectorate that we might be able to help with.

Lauren KATHAGE: Thank you. You spoke there about sharing information between agencies, but in terms of councils sharing information publicly I think you said one of your training resources was around the public sharing of information. Is that correct?

Sean MORRISON: It is around councils' obligation. Under the *Local Government Act* they have got an obligation to be open and transparent, and our resources is about how that combines with the *Freedom of Information Act* so councils can proactively release information rather than making people go through a request.

Lauren KATHAGE: Is this the push and pull?

Sean MORRISON: It is a mid-house. At the moment we have got our pull; we want our push. This is basically saying, 'Well, you don't have to wait for changes in the legislation. You have your obligations under section 125 around transparency under the *Local Government Act*, and this is how it interacts with freedom of information. You should be putting more information out there, and this is how you can do it.'

Lauren KATHAGE: Are there some examples of the benefits of the increased transparency by councils that you can see in terms of reducing the risk of fraud and corruption?

Sean MORRISON: Some of the themes we get around FOI requests are concerning spend or councillors' actions or things around enforcement. I think we all know that where there is transparency, there is a reduction – just anecdotally, and on some research – in fraud and corruption. Transparency is a fraud and corruption control, so the more information that is available, the harder it is to hide from detection an act that could be fraud.

Lauren KATHAGE: In the humanitarian aid space that I used to be in transparency was very explicit. There used to be signboards posted up in villages to say what was funded and what the scope was so that people could see if it was or was not happening and make sure that local government was using the money as it was given. So it is good that we can see all the different ways that transparency can help, so thank you.

You have spoken a bit about the shared services between councils and some of the benefits of that, but in terms of the role of the bigger councils as opposed to smaller councils in sharing expertise, there has been some discussion today about standardised frameworks for fraud and corruption control. In terms of information and the remit of your office, what would your view be on a standardised approach across all councils?

Sean MORRISON: For fraud and corruption, for information security or both?

Lauren KATHAGE: Information security as it relates to fraud and corruption.

Sean MORRISON: Again, if councils are subject to part 4, the controls in part 4 in our framework really assist in combating fraud and corruption. We go back to, there is physical security – have people been vetted before the role, so have they accessed information from things like security clearance checks? There are offboarding protocols as well – are people offboarded appropriately? There is actual physical security of the information – can the information be manipulated in a physical environment? So a standardised framework would assist all councils in combating fraud and corruption, because that is what our framework does.

Lauren KATHAGE: Thank you, Chair.

The CHAIR: Thank you, Ms Kathage. Mr Hilakari.

Mathew HILAKARI: Thank you so much for your attendance this afternoon. We have heard evidence that at some councils one in 10 decisions are made in confidential meetings; at some, according to the data, one in three almost are made in confidential meetings. Is this acceptable, this level of the use of confidential decisions put in place?

Sean MORRISON: I cannot –

Mathew HILAKARI: Particularly where some councils – interface councils – facing similar situations are as low as 1 per cent.

Sean MORRISON: I think OVIC's position is that the more transparency we have, the better, and if the recommendations we made to the Integrity and Oversight Committee were upheld, I think you would see that practice change where only the things that are of the highest public interest to maintain confidentiality and secrecy would be upheld.

Mathew HILAKARI: So what are the sorts of things that should be in that confidential area, as opposed to really opened up for the public to scrutinise and make their own choices on?

Sean MORRISON: I think personal information, particularly around someone's health care or disciplinary or anything like that – anything to do with enforcement, and I mean the very, very critical parts of enforcement, not a manual to do with parking infringements. Anything to do with national security or corruption frameworks, potentially, and anything that would really affect a council's position – say it was to do with contracting or a tender, and you would not want that information released beforehand. But it is a very limited subset, and there still has to be a public interest overlay test to that.

Mathew HILAKARI: Does your office have the capacity to look at those confidential decisions that have been made, or is this a power that you think would be appropriate?

Sean MORRISON: Always I would say – well, first, we do not have the power to look at it. I would have to see the numbers and potentially the scope of funding, because as we know –

Mathew HILAKARI: That is a well thought out answer.

Sean MORRISON: Yes. If there is funding, I am definitely happy to look at it.

Mathew HILAKARI: Okay. And if there was, I guess, one thing that you could do to change the systems in Victoria – I am guessing I know the answer to this from your submission already – what would that be to ensure that there is greater transparency, but also prevention of fraud and corruption?

Sean MORRISON: I will not say part 4. I will say –

Mathew HILAKARI: Oh, okay – you have shocked me here.

Sean MORRISON: Well, it was obvious, but I think mandatory reporting would really assist.

Mathew HILAKARI: In what way?

Sean MORRISON: Well, I think it brings Victoria into line with other jurisdictions, and so practitioners are aware of that framework already. It provides some information to the public so they are aware, but it also provides for a requirement for councils to inform the people when there is going to be serious harm from a security incident. It shifts away a little bit from the corruption and fraud framework to best practice with minimising harm, but also when you are dealing with a council, you know what their information security regime is like, so you can choose to share less information if you are oversharing, for example, and it creates a level playing field.

Mathew HILAKARI: Thank you. That is the time.

Sean MORRISON: Thank you.

The CHAIR: Mr Morrison, thank you so much for appearing before the committee this afternoon. We really do appreciate it.

The committee or secretariat may have some follow-up questions after today's hearing, and if this is the case, you will be contacted. Any questions taken on notice in writing require your response to be provided within five working days of the committee's request.

I would like to thank everyone who has given evidence to the committee today, as well as Hansard, the committee secretariat and parliamentary attendants. I would also like to thank the hospitality, security and cleaning staff who have looked after all of us today. I declare this hearing adjourned.

Committee adjourned.