COMMONWEALTH OF AUSTRALIA

# Proof Committee Hansard

## PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

**Security Legislation Amendment (Critical Infrastructure Bill) 2020 and Security of Critical Infrastructure Act 2018**

(Public)

FRIDAY, 11 JUNE 2021

CANBERRA



BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

**[PROOF COPY]**

**INTERNET**

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

To search the parliamentary database, go to:

**http://parlinfo.aph.gov.au**

**PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY**

**Friday, 11 June 2021**

**Members in attendance:** Senators Fawcett [by audio link], Keneally [by video link], Paterson and Dr Aly [by video link], Mr Dreyfus [by audio link], Mr Tim Wilson [by audio link].

## Terms of Reference for the Inquiry:

To inquire into and report on:

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) has commenced reviews into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and the operation, effectiveness and implications of the *Security of Critical Infrastructure Act 2018*. The bill review was referred to the Committee by the Hon Christian Porter MP, Attorney-General.

## WITNESSES

**FINCH, Ms Shannon, Member, Corporations Committee, Business Law Section, Law Council of Australia [by video link]**

**GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia [by video link]**

**MOLT, Dr Natasha, Director of Policy, Policy Division, Law Council of Australia [by video link]**

**NEAL, Dr David, SC, Co-Chair, National Criminal Law Committee, Law Council of Australia [by video link]**

**Committee met at 09:30**

**CHAIR (Senator Paterson):** I declare open this hearing of the Parliamentary Joint Committee on Intelligence and Security for its review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018. These are public proceedings, although the committee may agree to a request to hear evidence in camera or may determine that certain evidence should be heard in camera. In acknowledgement of the current COVID-19 situation, certain measures have been implemented, which will be self-evident to you. I remind all witnesses that, in giving evidence to the committee, they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated by the parliament as a contempt.

In accordance with the committee's resolutions of 4 July 2019, this hearing will be broadcast on the parliament's website and a proof and official transcript of proceedings will be published on the parliament's website. I now welcome representatives of the Law Council of Australia to give evidence at this public hearing today. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and, therefore, has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make a brief opening statement before we proceed to discussion and questions. I would ask you to keep opening statements brief so that we can reserve plenty of time for discussion.

**Ms Finch:** I will give an opening statement on behalf of all of the Law Council witnesses. The Law Council of Australia welcomes the opportunity to appear before the committee regarding its inquiry into the Security Legislation Amendment (Critical Infrastructure) Bill 2020. The Law Council acknowledges that the overall objective of the bill is to create a comprehensive national regulatory framework for the security of critical infrastructure across all sectors of the economy, which focuses on building resilience against attack or compromise. We also acknowledge the reasons for the regulatory focus on cybersecurity, given the interconnected technological environment in which most businesses operate. In the extrinsic materials to the bill, the government has noted its overarching intention to ensure that the regulatory burden of the new regime is no greater than is necessary and that proportionate approaches to enforcement are measured and risk informed.

While this broad statement of policy intent is welcome, the Law Council is concerned that it is not given adequate legal effect in the detailed provisions of the bill. The effective operation of the expanded regime requires the governing legislative framework to entrench core principles of transparency, clarity and certainty in the substance of regulatory obligations. The governing legislative framework also needs to drive efficiency in regulatory decision-making and offer comprehensive assurance to regulated entities that they will not be exposed to legal risk as a result of their compliance with their obligations. It is important that the primary legislation establishing the new regime contain adequate legal safeguards which require the regime to operate in a targeted, proportionate and accountable way.

Presently, we are concerned that the bill would leave this outcome substantially to executive discretion at the point of deciding how to exercise the broad delegations of the power proposed. We have made 40 recommendations for targeted improvements, which are directed to three key areas. In relation to the proposals to expand security obligations in new parts 2A, 2B and 2C of the act, we have made 11 recommendations, Nos 1 to 11, which seek to impose stronger and clearer statutory parameters on the exercise of powers by the Minister for Home Affairs, the departmental secretary and staff to determine the application and substance of regulatory obligations.

We have also made suggestions to better deal with interactions between the expanded regime and foreign investment, privacy laws and other laws applicable to regulated sectors or entities. Secondly, we have identified some potentially unintended instances in which the bill does not provide the degree of legal protection to

regulated entities that is necessary to give them assurance and confidence in operating under the expanded regime. In particular, our recommendation 34 seeks to address the fact that the bill does not confer immunities from legal liability on all of the individual personnel of regulated entities who act in compliance with their obligations. Our recommendation 37 seeks to address the fact that the bill does not contain clear provisions to manage the interaction of entities' regulatory obligations under the act with their pre-existing contractual obligations, especially under cyber insurance contracts. It is possible that these two sets of obligations may conflict and, in the worst case, compliance with statutory SOCI obligations may cause an entity to breach its obligations under an insurance contract or other contract.

Section 11CD of the Banking Act 1959 contains provisions to manage this risk under that regulatory regime and sets out that the SOCI Act should include a similar provision. Thirdly, we have made a further 11 recommendations, Nos 12 to 23, directed to the extraordinary ministerial authorisation regime in new part 3A of the SOCI Act, which will enable the government to intervene unilaterally in responding to cybersecurity incidents affecting certain privately owned assets. Our recommendations would address several instances of overbreadth and imprecision in the scope, thresholds and authorisation process for this novel power and associated legal immunities for Commonwealth officers.

Before I conclude our opening statement, I note that the chair of our foreign investment committee is unfortunately an apology this morning. There may be questions that your committee has that will need to be taken on notice, and we will respond to those as well as we can. Thank you, Chair and committee members. We're happy to answer your questions.

**CHAIR:** Thank you very much, Ms Finch and all witnesses from the Law Council, for your engagement on this substantive bill and for the significant number of regulations that you have proposed. I will ask an initial question or two and then offer the call to my colleagues. Ms Finch, in your opening statement, you said that the Law Council recognises the need for this legislation. If the government adopted the majority or at least the most significant proportion of the recommendations that you make, would the Law Council support the passage of the legislation?

**Ms Finch:** Yes, I believe that we would. We recognise the critical significance of this piece of legislation and the factors that are driving it. Our concern is to make sure that the regime is balanced, has appropriate guide rails and oversight structures and is workable for business.

**CHAIR:** Would it be fair to say that a theme of your feedback to the government is your concern in a number of different areas about the amount of discretion that is left to the executive and that you would like the parliament to be more restrictive in the freedom given to the executive to implement the legislation?

**Ms Finch:** That's correct. We recognise that there are some instances in which the government has to be able to move swiftly to exercise some of the powers under this bill. But there need to be checks and balances and the opportunity for oversight, and the broad powers should be restricted to use in emergency circumstances. When it is not an emergency circumstance, there needs to be a more measured approach, with more transparency and opportunities for engagement.

**CHAIR:** I'm interested in these emergency circumstances because you and other submitters have raised some concerns about the step-in powers to be granted to the ASD in the event of a significant attack. What are your suggestions as to how those provisions could be improved?

**Ms Finch:** Dr Neal, this might be a question for you.

**Dr Neal:** In principle, the primary point is in relation to the authorisation power. You will see in our submission that we have referred to the recommendation of the INSLM that the authorisation power should go to an external source; and the recommendation that the INSLM has suggested is the specialist arm of the AAT, where there would be a judge experienced in security matters who could deal with these authorisations. That, we think, would be a very important principle in order to ensure that there is some degree of external oversight in relation to the issuing of the ministerial authorisations, the directions and the other aspects of the scheme, and then there are some other issues throughout. For instance, we would say that the role of the Inspector-General of Security in the issuing process shouldn't rest with IGIS. In the line of accountability, IGIS is there to oversee the operations of the various security divisions that it oversees; and, if it becomes involved in the issuing process, it would be in the awkward position of investigating its own activities.

To respond at the general level to your inquiries about the issue of the oversight and external scrutiny of the operational aspects of the scheme, they are two points that we would highlight. Then, in relation to section 3A

contained in the submissions, there are some more matters of detail. Beyond what's in the submissions, there are some more matters of detail that probably require some more scrutiny too. For instance, regarding the powers of the ASD to become involved in the operations, there is a restriction, for instance, on the responsible entity taking offensive actions in relation to the computers that it's using. The prohibition on taking offensive action, in section 35AB(9), applies to the entity whose machinery is taken over, but we don't find an explicit restriction on the ASD taking offensive action.

We applaud the general intent of the bill, which is to prevent offensive action being taken, and we certainly approve of that being prohibited in relation to the responsible entity. But it also should be explicitly prohibited against the ASD doing anything similar to that, and we don't see that explicitly in the bill. It may be implicit or buried somewhere, but section 35AB(9) explicitly restricts it to the entity and doesn't take it a further step and restrict the ASD in most of those respects.

**Dr Molt:** Just to add to what Dr Neal has stated there, we've also made recommendations in relation to the thresholds. For example, under sections 51 and 52B, which enable the minister to make declarations privately for critical infrastructure assets or matters of national significance, we have suggested that that should only occur where the minister is satisfied on reasonable grounds that there is a significant risk of harm to Australia's defence or national security as a result of the disclosure of the regulatory status of the asset. So, just to reiterate what Ms Finch and Dr Neal have stated, some tightening of the thresholds throughout the legislation can certainly ensure that it's more proportionate to the policy intent.

**CHAIR:** This is probably more back to Dr Neal's point than yours, Dr Molt. In particular, in relation to the ASD step-in powers, in the event of a crisis, it's quite likely that extremely rapid action will be necessary to address this. It's a crude analogy, but it's been put to me that when a building is on fire and the fire brigade turns up you don't debate with the fire brigade whether it's necessary to turn on the hoses and start putting out the fire; you put out the fire and have a discussion afterwards about what the consequences of that were. In some of these instances, are we really going to have time to litigate with the ASD about whether it's necessary for it to jump on the system and defeat an attacker or protect a system?

**Dr Neal:** I don't think it's so much that; it's the ministerial authorisation power that I was referring to. It's pretty common in the law for emergency warrants to do various things and they can be and are obtained over the telephone. The real point was to shift the authorisation, which would be required in the emergency situation as well, from the minister to the AAT specialist division. As for the level of external scrutiny, which I was responding to in relation to your question, we think it's too in-house, as it presently sits with the secretary and the Minister for Home Affairs.

**CHAIR:** Understood. Senator Keneally.

**Senator KENEALLY:** I like that analogy from the Chair. I suppose, if we take it a bit further, your argument seems to be that, when the fire brigade is sent out, the Minister for Emergency Services isn't consulted; it's the experts who take the decision to send out the fire brigade. Would that be a fair assumption; would that be a fair characterisation of your argument?

**Dr Molt:** I think the key issue is that, really, the difficulty with this legislative framework is that there's no gradation, in terms of going to a business or a company and saying, 'We've got this situation; we need assistance from you to help resolve it.' Instead, it seeks to go to a 'stick' approach right from the beginning with business, where businesses have to comply with the regime on pain of, for example, a civil penalty, if they don't. That is in contrast to other legislation that we see, such as the encryption laws, where there is more of a gradation approach and agencies can seek requests, for example, from businesses, and there is that opportunity for businesses to be able to comply voluntarily. So, just going back to your situation where there's a fire, normally when that occurs and you have firemen or firewomen coming to a building to put out a fire, businesses volunteer, 'Yes, we're more than happy for you to help.' But this situation isn't comparable because businesses are not actually being given a chance to volunteer assistance.

**Senator KENEALLY:** At the risk of stretching the analogy too far, it does strikes me though that, if we're going to use the fire analogy, government have regulations, in terms of building safety codes and the like, in order to limit the impacts of fires. Wouldn't it be fair to say that what the government is seeking to do here, with the regime and the obligations on businesses to have certain measures in place, is to require a business to put in place security measures before a fire erupts. From your submission, I take it that you don't object overly to that approach of putting a positive requirement on businesses to put certain measures in place. It goes back to the chair's question about supporting the intent of the legislation.

**Ms Finch:** That's right. I think, in general, we acknowledge the logic of having an obligation for companies to put some measures in place. There is an interesting parallel with the Securities Commission's approach, in looking at this from the perspective of directors' duties and regarding it as being a matter of directors' duties to ensure that there are measures taken around cybersecurity so that it is in line with broader policy objectives as to prudent management of businesses. The core principle is fine; it's the question of whether it's taken to extremes. So, again, probably stretching the analogy beyond its intent, having the emergency services rush in and offer assistance in the first hours of a fire is great. If the fire keeps burning for a matter of months—sometimes these incidents can involve protracted periods of engagement from cybersecurity incidents that we've seen already—there has to be a role for businesses to have a voice and some involvement in how the strategy affects them. I don't think it's a simple matter of saying that it's an emergency service and these officers who are engaging in this intervention will necessarily understand all of the nuances of the impact on the businesses and be able to make the right judgement; there has to be an interplay with the governance systems of the businesses.

**Senator KENEALLY:** Actually, I have three questions that arise from reading your submission; and I know that other colleagues may have questions as well so I will try to move through those questions. One does go to that last point that you just raised. Your submission notes where immunity from liability is inadequately expressed in the bill, including for ASD officers and personnel of regulated entities. This issue has come up in some of the submissions from, particularly, operators of critical infrastructure and essential services, where they are seeking immunity, particularly for directors, if companies or organisations follow government direction and subsequently it turns out that there is a bad outcome for shareholders. Can you just expand a little bit and, in particular, comment on that issue about immunity for directors, given the assertion from operators and other businesses that there's now going to be a conflict between the Corporations Act and the obligations for directors, potentially, with the government step-in powers?

**Ms Finch:** Certainly. We have to assume that, in exercising its powers under this legislation, the agency's concerns will primarily be the national interest; it is not its responsibility to be looking out for the interests of shareholders; so there is always the possibility that the measures that are considered to be in the national interest will, in fact, be to the detriment of the business and to the detriment of its investors. That is something that, I think we accept, is part of the price of managing the scale of the risk, which the government is trying to address here; however, it has to be tempered with the impact upon the businesses and the individuals who are managing those businesses. If they are to embrace a situation where they cannot have an influence and their view is not the deciding view as to the way forward or the way to address a particular crisis, there has to be some protection for them against allegations of a breach of duty in circumstances where they have no opportunity to exercise their duties.

**Senator KENEALLY:** Just in the interests of time and being mindful that we've got a full day here, I might ask you, on notice, if you have any particular recommendation about how that might be dealt with legislatively. Throughout your submission, you have identified specified terms that are overly broad, overlapping or at odds with existing legislation; for example, what constitutes a cybersecurity incident of 'relevant impact', 'national security' or 'offensive cyber action'. Can you discuss some of those examples and just say what the impact is of having broad terms or undefined terms in the legislation?

**Ms Ganopolsky:** I'm happy to expand on some of those examples, if I may. They are covered in the submission and go to a number of recommendations. But the critical issue is that the bill, with the way it's drafted, has created two distinct lines of incidents. Under section 30BC, you have a cybersecurity incident that is critical, and what is 'critical' is not defined. Under section 30BD, you also have a cybersecurity incident, and you have a general obligation in respect of those types of incidents as to what is 'relevant impact'; that's a very broad definition of what is relevant, with no issue of materiality. So you've got these two obligations that use different language. Some points of materiality are used in a way that is not expanded upon or defined by any legislative means, and you just have to go to the colloquial, natural English-language meaning of it, but both create reporting obligations. However, if it's a critical cybersecurity incident and, therefore, you have more extreme circumstances perhaps, the explanatory memorandum gives some colour to that, but none of that colour is reflected in that notion of criticality, which seems to be repeated in the last proposed sections. Again, if you then contrast it back to the provisions of proposed section 30BD, anything could be relevant and, again, there is no materiality on that issue of relevance. So, apart from the fact that the concept of a cybersecurity incident is defined in section 12M, you then have these potentially divergent paths. That is a practical matter that needs to be fixed well before you get to some of the examples that we have already discussed under part 3A of the act, where you've got 'intervention'.

These are ongoing obligations by organisations. Some organisations already have obligations around cybersecurity, and they work to definitions and regulatory regimes: APRA regulated entities and CPS 234, to

name just a couple of examples. But there's an expanded economy-wide set of ongoing, daily obligations to provide certain reports, and this is entirely unworkable. It's more than a question about being unworkable because it's inconvenient or time-consuming. I think everybody accepts that this is an important area. This actually goes to the stability of the very regime that is being set up and invites so many unintended consequences that actually will detract from the efficiency of organisations having appropriate corporate governance around these matters, appropriate reporting for these matters, appropriate escalation of these matters and, actually, some form of uniformity. That, again, goes back to information sharing and some of the policy objectives that notification regimes are designed to serve. So, in our view, it would be critical to observe this as a matter of housekeeping for organisations. But it goes to the core of this daily interaction that this regime sets up economy-wide for some highly regulated industries and some yet to come into the fold; and, in practical reality, it is unworkable.

**Ms Finch:** I would say that it is not that we do not appreciate the thinking behind having broad powers and broad concepts in terms of that ability to adapt to particular contexts and circumstances, but we have seen the effect of this sort of uncertainty and complexity and these sorts of broad-reaching definitions in other sector regulation. One that stands out the most is probably financial services. What we find is that it does not lead to effective compliance. That's not to say that you have to have a set of highly prescriptive tick-box rules, but you do need very clear guide rails for businesses to comply with it. Also, in order to support their reporting, you also need to develop systems that mean the default compliance or the default steps, more likely than not, cause them to be in compliance. This shouldn't be a regime that's set up to have gotcha moments for business; it should be something where the regime supports compliance.

**Senator KENEALLY:** Chair, I might have some other questions but I'm conscious of time and the need to share the call around, which I'm happy to do at this point. If there's time later, I will come back.

**CHAIR:** I just want to revisit one of the issues raised by Senator Keneally in her line of questioning. Then I will invite another coalition colleague to ask questions, in the event that they have some, after which I'll see whether Mr Dreyfus or any other Labor colleague has any. Dr Molt, in response to Senator Keneally, I heard you say that businesses should have an opportunity to cooperate and comply voluntarily before being obliged to do so or before heavy-handed step-in powers are used. Do you have a sense of the extent to which businesses are currently cooperating with government on these issues? For example, when they suffer a cyberattack, how open and receptive are they to assistance?

**Dr Molt:** That's probably a question that Shannon Finch is best placed to answer. But I think, anecdotally, from what we've heard, businesses are generally very receptive and cooperative with government.

**Ms Finch:** I think that's right. I think the response of businesses to cyber incidents has been pragmatic; if there is assistance and guidance available, they will gratefully take it. I think there's some tension with other parts of the regulatory system at the present time. Where we have the Securities Commission indicating that a lack of preparedness for cybersecurity incidents may be a breach of directors' duties, you may derive there being a reluctance of business to engage with the Securities Commission around the incident that has occurred because it may increase exposure to investigation and cost. I think this is one of those circumstances where the scale of the problem should drive a rule-of-government approach where regulatory agencies are aligned around core objectives, which then defends and supports businesses against these sorts of attacks and allows us to have a united national approach, as I say, identifying points where businesses have failed. If you do take that approach, business will be very cooperative.

**CHAIR:** Would it change your views at all, if you were aware that there were businesses failing to cooperate and refusing assistance?

**Ms Finch:** No, it doesn't change my view as to the design. I think you have to create an environment that encourages engagement and cooperation. A simple big-stick approach will not do that. It will send businesses into defensive positions, in which they will be reluctant to communicate; and what you want here is communication and a cooperative approach.

**CHAIR:** I might explore this with Home Affairs later and the ASD, to the extent that it's able to talk about it. But I'm aware of at least one instance where a systemically important major Australian business suffering a cyberattack was not cooperative with government when assistance was offered; it declined assistance.

**Ms Finch:** Do you have any visibility as to the rationale for that?

**CHAIR:** No, I don't. That's something that we will explore with Home Affairs.

**Ms Finch:** I think that's the start of the question. Where government appears to have something to offer and where assistance could be valuable, you have to ask the question, 'What was it that deterred that business from seeking and embracing that assistance?'

**CHAIR:** That's a very good question, and we will pursue it. Senator Fawcett.

**Senator FAWCETT:** I'm just interested in a view of the Law Council. The evolution of this legislation has gone from critical infrastructure in utilities—things like power, water and gas, et cetera—to, in its expansion, looking at systems; and Home Affairs, in paragraph 64, talks about the 'dynamic cascading threats' that are enabled by malicious cyber activity. That overlaps, to a large extent, with some of the work that's currently going on with supply chain resilience. In one of the other committees of the parliament we heard from, for example, the pharmaceuticals industry, which talked about the risk to the health system of disruption to pharmaceuticals in the supply chain. APIs are disrupted, then a limited number of manufacturers become disrupted and then Australia starts missing out on critical medications for its population. I'm just wondering about the Law Council's view about the framework that's being established here, predominantly in the context of a cyber security resilience, and whether you think it could be expanded or would be problematic to expand it, to areas that are of national significance, in requiring companies also to have plans around supply chain resilience.

**Ms Finch:** Unless one of my colleagues wishes to respond, perhaps we can take that question on notice and get you a response that addresses a range of stakeholders. It's a very good question, and I think there are a number of stakeholders in the Law Council who would wish to have an opportunity to contribute to the response.

**Dr Molt:** Perhaps I might just add that the Law Council is certainly not opposed to the proposed expansion to the 11 proposed areas. I think, though, it just comes down to what we've been isolating, which is how that is expanded and how the regime is proposed to work.

**Senator FAWCETT:** I guess the key point is that, as we expand this to include the health system, it's all very well to protect a hospital; but if, for example, pharmaceuticals aren't available, the health system as a whole will become compromised and, if that's going to be part of a critical national system, perhaps we should also have ongoing interaction with industry around how that supply chain resilience is framed.

**CHAIR:** We'll go to Mr Dreyfus.

**Mr DREYFUS:** I thank the Law Council, yet again, for a tremendous piece of work, with a comprehensive review of the existing legislation and this bill. Obviously, I don't have time to explore the detail, but I don't need to, because you've gone to considerable trouble. I just want to ask you to expand on what the Law Council has said about the linked topic of limitations on judicial review rights and the absence of merits review rights. Just by way of introduction, as I understand it, this is, I presume, a very familiar theme for the Law Council and something that comes up quite often. But you're concerned about the exclusion of decisions from judicial review and about the absence of merits review in respect of certain decisions. Perhaps I could ask you to expand on that?

**Dr Molt:** The bill, as set out currently, proposes to exclude administrative decisions from judicial review under the ADJR Act, particularly part 3A of the bill. Also, no proposed merits review is available for these decisions either. The Law Council considers and has made recommendations that both judicial review under the ADJR Act and also merits review should be considered. The approach that the bill seems to take is that, given that some of these decisions may involve sensitive information relating to national security, which we appreciate, there's a blanket approach to ensuring that the ADJR Act and merits review is not available. We need recommendations about, again, making that a more targeted system.

For example: with the approach that we've taken to merits review, there is the Security Appeals Division of the Administrative Appeals Tribunal, which already and currently has the facilities and capability to deal with sensitive information. We do think that merits review is important to allow the entities affected by these administrative decisions some kind of recourse. At the moment, for example, there is very little ability in the bill for entities that are affected to go through a conflict resolution process; that's not available. So, as a minimum, at the back end of it, we consider that statutory judicial review and merits review are important.

**Dr Neal:** Perhaps I could add to that answer and take up a point made earlier, which was about encouraging confidence in businesses to cooperate regarding these issues. At the moment, in part 3A, there's the power of the Australian Signals Directorate to come in and alter, change or delete information on the entity's computers; that does not seem to be accompanied by an obligation to provide the entity with information about exactly what has been done to their computers. I'm presently involved in a case where a company's computers have been tied up for months, not because of a security issue but other issues, and the company still hasn't got those computers back. This comes up acutely in the area of 3A, which is premised on the basis that the corporation is not prepared to cooperate. But if there were a more cooperative spirit in that section of the legislation, which provided information to the business concerned about just exactly what was required to be done and was done, it might engender more confidence, apart from being fair.

Similarly, with the power to review decisions, where Home Affairs has misconceived the nature of the problem or the nature of the data that it's dealing with—that arises particularly where the organisations concerned have very sophisticated systems—you can understand why those organisations would be concerned about people coming in and playing around with their staff when, firstly, they're not going to be told exactly what was done and, secondly, their opportunity to challenge it is also removed. I think it's dangerous to have so much confidence in one entity which is not subject to external reviews at the input of compulsory powers, during them or after they've been done.

**Ms Finch:** I might add to that. There is also a lens to that, remembering the picture of Australia facing out to the rest of the world. The corporations committee often looks at this from the perspective of what impact there is on our participation in global markets and the ability of Australian businesses to seek investment from other markets and do business across jurisdictions. As it is, the Australian regulatory regime often takes other major markets by surprise. Having said that, one of the most powerful factors around attracting investment to Australia is the rule of law and the balance in our regulatory regimes. So, to the extent that we grant broad powers like this, there has to be a visible system of checks and balances as well as opportunities for oversights and review.

**Senator KENEALLY:** Can I jump in here, Mark, if you don't mind? I have a follow-up on this specific point.

**Mr DREYFUS:** Of course, yes.

**Senator KENEALLY:** Thank you. The Business Council of Australia and some other entities that have made submissions—I think the Australian Banking Association had done so as well—have argued this very point about a significant power being vested in the hands of one entity. They have made a recommendation that the relevant regulator for those industries or sectors—say, an APRA, ASIC or ACCC—should be consulted as well, before that type of step-in power is enacted. I don't know whether you've seen that recommendation—I'm happy for you to take this on notice—but I wonder whether you have a view about what regulatory regime for that industry or sector would be an appropriate check or balance.

**Ms Finch:** By itself I don't think it's sufficient. I would endorse that view, particularly in the case of APRA. If you can imagine a step-in right being used where there can be interference with systems in banks that could go to the stability of those organisations, that is absolutely of systemic importance; and that is APRA's job, to be the guardian of stability of our financial system. It is inconceivable that a step-in power like this could be exercised in the financial services sector, without the engagement of APRA. But perhaps we might take that question on notice as it applies more broadly.

**Mr DREYFUS:** Just to go back to where we were: I'm pleased that you've mentioned the rule of law. Mr Morrison has spoken about the rule of law repeatedly over the course of this year. With Australia being a sophisticated country, I'd hope that rule-of-law principles would apply particularly to complex regimes, such as a 'security of critical infrastructure' regime. Just on this question of the use of the ADJR Act and the application of the principles expounded by the former Administrative Review Council, could one of you speak to what you've said in paragraph 269 of your submission. That paragraph simply makes the point that, while it's not open to this or any other government to exclude judicial review entirely, there are limitations on that constitutionally preserved right of judicial review.

**Dr Molt:** If I heard you correctly, your references go to paragraph 269 of our submission. We set out there the difference between statutory judicial review compared to judicial review under the Constitution. One of the primary differences is the absence of a statutory right to reasons under the constitutional judicial review mechanism. Also, just to elaborate further on that, the benefit of the ADJR Act is really that it provides a simplified form of access to judicial review, which in this context, in particular, is particularly valuable when you're dealing with Australian businesses, for example, that want a relatively straightforward remedy or at least the ability to contest that.

**Mr DREYFUS:** I've got one other matter, which goes to an impacted section of the submission dealing with independent operational oversight. We've got the Ombudsman and the Inspector-General of Intelligence and Security coming to speak to us next, after you, but I invite the Law Council to expand on the concerns that you've expressed about the role of the Commonwealth Ombudsman, under the bill, and the crossover with the role of the Inspector-General. In essence, do you believe that the operational oversight in the current bill is adequate?

**Dr Molt:** There are some difficulties regarding the proposed oversight by the Commonwealth Ombudsman when compared to, for example, IGIS. One key example of that relates to the proposed secrecy offences. Currently, under the Security of Critical Infrastructure Act, there's a secrecy offence provision in section 47 of that act. That requires, for example, that except where it is necessary to do so for the purposes of giving effect to this act an entity is not to be required to disclose protected information or produce a document containing

protected information to a court or a tribunal. There is proposed in this bill an exception for authorised disclosure, for example, to the Inspector-General of Intelligence and Security, but there is no corresponding exception for entities to provide information to the Commonwealth Ombudsman. We consider that also makes it difficult, in terms of any information sharing between both the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security.

**Mr DREYFUS:** I've got nothing further, Chair, but I would, again, thank the Law Council for the comprehensiveness of the submission.

**CHAIR:** Do any colleagues have further questions? Senator Keneally, you flagged that you may have a number to follow up on.

**Senator KENEALLY:** On the issue of oversight, I do wonder if you've turned your mind to whether this committee should have any particular role in relation to oversight. For example, there are many pieces of legislation where the PJCIS is briefed on an exercise of a particular power—citizenship loss, for example. Have you turned your mind to whether this committee should have some ongoing oversight responsibility, in relation to the exercise of the powers under this act?

**Dr Molt:** Yes, we have. In terms of the ongoing review, in recommendation 31, which is on page 87 of our submission, we have recommended that there be independent review, for example, by the Independent National Security Legislation Monitor and also subsequent review by this committee, considering, for example, the findings of the INSLM.

**Senator KENEALLY:** I think some of the other witnesses that we'll have at subsequent hearings may make an argument that this committee should be briefed, if a step-in power is exercised, in the way that we are briefed on other aspects of national security legislation when extraordinary powers are exercised. I'm happy for you to take that on notice. But I'm just curious about what role this committee could play, in terms of representing the parliament, in receiving information about the exercise of powers.

**Dr Molt:** We can take that on notice. I think in our submission we have outlined that we would support parliamentary oversight, for example, when the minister chooses to make a declaration in certain circumstances. But, yes, we can provide more information on that on notice.

**Senator KENEALLY:** I did want to come back to the interaction with foreign investment laws, because this is an issue that, again I anticipate, we'll be hearing about from other submitters in other hearings. Can you just flesh out for us a bit more how the proposed delegation powers have broader implications for proposed foreign investments in relation to critical infrastructure assets?

**Ms Finch:** We may need to take your questions on notice around foreign investment, as the chair of that committee was unable to attend today.

**Senator KENEALLY:** That's okay.

**Ms Finch:** With foreign investment, there is always an intensely practical lens. Foreign investment questions and reviews arise in the context of transactions, so the ability to have transparency around processes and timing and to have opportunities for engagement—even if that must be on a strictly confidential basis—is absolutely critical to the functioning of the interaction of this regime with the foreign investment regimes. We have a specialist committee dedicated to that very question. So, if you have any questions, please let us know, and we will answer them in writing.

**Senator KENEALLY:** Thank you; we will. As I've said, some of the other submitters, particularly from industry, have raised these concerns, so we may do that after subsequent hearings.

**CHAIR:** As there are no further questions from committee members, I thank the representatives of the Law Council very much for their attendance and evidence before the committee today. We're grateful for your assistance. We would be even more grateful if you could return the questions you took on notice to the secretariat by Friday, 25 June so that we can complete our report. As usual, as you'd be familiar with, you will be sent a transcript of your evidence in draft form in case you would like to suggest corrections to any transcription errors; otherwise, thank you very much for your time this morning.

**Ms Finch:** Thank you, Chair, and thank you, Senators.

**FALLEN, Mr Brad, Acting Assistant Inspector-General, Office of the Inspector-General of Intelligence and Security**

**FINTAN, Mr David, Senior Assistant Ombudsman, Strategy Branch, Office of the Commonwealth Ombudsman**

**JESSUP, the Hon. Dr Christopher, QC, Inspector-General, Office of the Inspector-General of Intelligence and Security**

**McFARLANE, Mr Steve, Assistant Inspector-General, Office of the Inspector-General of Intelligence and Security**

**McKAY, Ms Penny, Deputy Ombudsman, Office of the Commonwealth Ombudsman**

**NOTZON-GLENN, Ms Bronwyn, Acting Deputy Inspector-General, Office of the Inspector-General of Intelligence and Security**

[10:25]

**CHAIR:** Welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and, therefore, has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. Does either organisation wish to make an opening statement?

**Ms McKay:** I have a short opening statement. I thank the committee for the opportunity to be here today to contribute to your review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020. The Ombudsman, Michael Manthorpe, sends his apologies; he had a personal commitment today. The Ombudsman's oversight role in relation to this bill is to have the ability to receive, consider, and take action in relation to any complaints made about two things: the Secretary of Home Affairs' use of the power to issue directions or make requests; and the AFP's actions in supporting the ASD under the power. This oversight role relies on our existing functions and oversight of the Department of Home Affairs and the AFP, and it proposes that we work alongside IGIS to oversee different aspects of the framework. Our interest in this review is to ensure that our ability to provide that oversight works as intended; and, to that end, we raise two points.

Firstly, as raised in our submission, we are concerned that the secrecy provisions, as currently drafted, may prevent someone from making a complaint to our office. This is because information about the making of a direction or request by the secretary would be included in the expanded definition of 'protected information', and it's an offence under section 45 of the act to disclose protected information. Currently, there is nothing in the bill that creates an exception for disclosure of such information to our office, and we would ask for that exception. Secondly, if we receive a complaint about the use of this power, it's important that we are able to obtain the necessary information and ask the necessary questions to be able to investigate the matter. Section 47 of the act currently provides that a person cannot be required to provide protected information to an authority with the power to request it. This bill proposes an exception to this provision for IGIS. We ask for a similar exception so that we can obtain the information that is required to investigate. We're pleased that the bill contains information-sharing provisions so that we can share protected information with IGIS, and vice-versa. Many of the submissions to the committee today go to the policy rationale of the bill; we don't propose to comment on those policy issues, but I'm happy to answer any questions that the committee might have today.

**CHAIR:** Dr Jessup, would you like to make an opening statement?

**Dr Jessup:** Yes, thank you. I thank the committee for inviting us to appear at today's hearing. I have a short opening statement. Firstly, I'd like to clarify that we are appearing before the committee as part of its review of the bill and not its statutory review of the Security of Critical Infrastructure Act; as such, IGIS currently does not have a direct role under that Act. IGIS's role under the bill is twofold. IGIS's primary role would be to review ASD's conduct under the framework for legality, propriety and compliance with human rights; this would be facilitated through IGIS's existing oversight jurisdiction, under the IGIS Act.

Secondly, the bill proposes that IGIS be provided with a new function to issue evidentiary certificates, setting out any facts relevant to the question of whether anything that ASD did was done under the authority of the act. The bill proposes that my office and the Commonwealth Ombudsman's Office will have oversight jurisdiction under different aspects of the framework. The bill contains information sharing provisions which will help to manage our complementary oversight jurisdictions. To assist the committee, my submission makes two substantive points about how the bill impacts my oversight. The first concerns the impact of the proposed

Intelligence Services Regulations. This matter is discussed in paragraphs 11 to 13 of my submission. The purpose of these regulations, as explained in the draft explanatory materials that accompany them, is to enable ASD to assist or cooperate with the Department of Home Affairs in the exercise of the department's powers and functions under the Security of Critical Infrastructure Act. However, as currently drafted, the draft regulations would enable ASD to cooperate with Home Affairs more broadly in respect of any of the department's functions. Clarity in relation to the precise scope of the assistance that the parliament intends ASD to provide to the department will assist IGIS in reviewing the legality and propriety of ASD's conduct.

The second matter discussed in my submission relates to information sharing and disclosures to my office; this matter is discussed at paragraphs 14 to 17 of my submission. Under the bill, there is no exemption for my staff to share protected information within the office; that is, for IGIS staff to share with IGIS staff. The bill also raises a number of policy matters that will be of interest to the committee. We have been consulted on the bill by the Department of Home Affairs, but we do not express a view on those policy matters. I would be happy to answer any questions that the committee might have.

**CHAIR:** I'll ask a couple of initial questions before I offer the call to my colleagues. I'm interested in the exceptions, which each of you have noted, that are lacking in the bill for each of your organisations. Firstly, Ms McKay, this is to you as Ombudsman. As I understand it, you are seeking two that are not in the bill: firstly, clarification that people can report to you; and, secondly, clarification that you can investigate. Has that feedback already been provided to Home Affairs and, if so, what response have they given you?

**Ms McKay:** We were consulted by Home Affairs, through the Attorney-General's Department, while this bill was being created. We did raise the first issue, which is the one relating to people being able to make complaints to our office. The second issue we have not raised, and that's why I raised it today in my opening statement.

**CHAIR:** We can put this to Home Affairs this afternoon, although we'll have a lot to put to them, so I'm interested in the insight that you can provide. Did Home Affairs think it was not necessary to have this clarification and that it was already clear or do you think this is an unintended oversight that Home Affairs would be willing to correct?

**Ms McKay:** I think it's probably the case of the latter rather than the former. I certainly haven't received feedback that it wasn't appropriate to make that amendment, so I would say that it was more in the latter category and was an unintended consequence.

**CHAIR:** It's an enormous and complex piece of legislation, so exactly what this parliamentary process is for is to identify things like that, but we will take that up either with Home Affairs this afternoon or in another capacity. Essentially, I'd ask the same question of IGIS about the exception that it's seeking. Have you previously raised that with Home Affairs and, if so, what was their response?

**Dr Jessup:** We have been consulted by Home Affairs. I'm unable to say whether it was specifically this point that was agitated with them, but no doubt you'll be able to clarify that with them.

**CHAIR:** Are any of your colleagues able to assist with that?

**Ms Notzon-Glenn:** Yes, we did have a number of consultations with the Department of Home Affairs. I suspect that it is—as you said, Chair—an unintended consequence that has arisen, and this is why we've raised it in our submission.

**CHAIR:** Equally, with the Ombudsman, Home Affairs hasn't said to you why it would be problematic to amend the bill in this way or said that it couldn't be done; it's just that it hasn't done so as yet?

**Ms Notzon-Glenn:** Yes. I suspect that it's just one of those things that has arisen and, as you've said, it's a very complex bill. Certainly, we can be part of further discussions with Home Affairs. The consultations were very extensive.

**CHAIR:** I have one other matter, and then I'll offer the call to others. I'm interested in the oversight responsibilities of ASD that, under the legislation, are contemplated for IGIS. Do you think it will be sufficient to scrutinise the activities of ASD that are proposed by this bill?

**Dr Jessup:** The oversight responsibilities that I would have don't arise directly under this legislation. Because ASD is the body that has the powers and functions under this legislation, we get oversight of that by reason of the IGIS Act itself. That is to say, we have oversight of all of the activities of ASD with respect to legality and propriety subject to the various exceptions that are set out in that act. This particular bill, as we understand it, doesn't introduce any new specific oversight functions. There is the certification function, which has been mentioned, but as far as oversight is concerned our role is activated because it happens to be ASD.

**CHAIR:** As we discussed with the Law Council, though, the bill does contemplate responsibilities for the minister and the secretary in authorising some of these actions. You don't have oversight of the minister or the secretary, do you?

**Dr Jessup:** No, we don't; and we don't have any role in relation to authorisation either.

**CHAIR:** Are you concerned at all that there wouldn't be an independent oversight mechanism for the minister and the secretary in their responsibilities under the act?

**Dr Jessup:** I'd prefer not to comment on that. As for the oversight, as a very high-level generalisation, IGIS exists because there are agencies which work within a very highly classified security space and, for that reason, their activities and reasons for taking those actions cannot be publicly visible. So IGIS is, if you like, a bridge between what they do in the classified space and the parliament and the community in the unclassified space. But if we were to have oversight of what the minister and the secretary of the department do, that would be a departure from that general principle.

**CHAIR:** Senator Keneally.

**Senator KENEALLY:** I thank IGIS and the Ombudsman for appearing today. I apologise, as I had a bit of a technical difficulty earlier and you may have covered this. Somewhat picking up on a similar point and directing this to IGIS, the Law Council of Australia in its submission has raised a concern that the thresholds for reporting ASD activities to IGIS were too high. Its submission argues that, as drafted, notification requirements are only activated if an ASD staff member would 'commit an offence but for the immunity provided by the bill or if ASD knows that its actions have caused material damage'. Do you hold similar concerns as those expressed by the Law Council?

**Dr Jessup:** Senator, could you draw my attention to that passage of the Law Council's submission?

**Senator KENEALLY:** I don't have that right here in front of me; I'm quoting from a question I drafted based on it. If it assists you, what I might do is provide that to you on notice.

**Dr Jessup:** Yes, I suppose so.

**Senator KENEALLY:** I'm happy to put this question on notice; that is fine.

**Dr Jessup:** Yes. The Law Council submissions are very comprehensive and in places—I would have to say, with respect—unnecessarily argumentative. Nonetheless, that's what they are; they're lawyers, so they work in that space. From my own background, I can say that lawyers always tend to read a document with a view to asking what's wrong with it. No doubt the committee gets a lot of assistance from them, but I think we'd be best taking that question on notice.

**Senator KENEALLY:** So, you will do that and we will organise for that to be done. I'll try this; I'll put this to the Commonwealth Ombudsman as well. The Law Council also suggested that the Ombudsman be notified of ministerial authorisations and have statutory inspection functions. Do you have any comment on that proposal?

**Ms McKay:** Yes. I would say, firstly, that the framework of oversight that's provided in this bill is a matter of policy for government, and I won't comment on that. I will say that we have many inspection regimes of law enforcement powers, but the common theme with those inspection regimes is that they are law enforcement powers that are used covertly so that the people who are subject to those powers don't necessarily know that they are being subjected to them. We have that inspection regime to be able to provide the oversight in that manner. These powers differ from those regimes in that the entities which will be subject to the directions from the secretary or the requests for intervention will be well aware that the powers are being used against them; therefore, being very much in a place where they can make a complaint to our office. So, it is a different kind of regime than we currently have inspection powers over.

**Senator KENEALLY:** Going back to the Law Council and 'being notified', are you saying that notification is not necessary, because people will be aware of the ministerial action, authorisations or otherwise?

**Ms McKay:** Yes. They will be aware and are in a position to be able to make a complaint to our office, which we can then investigate. Likewise, IGIS will also have a role where they will be able to provide us with information, should they wish to, under the information sharing powers.

**CHAIR:** Senator Fawcett.

**Senator FAWCETT:** The last sentence in paragraph 16 of the IGIS submission says, 'Disclosures between IGIS officials have not been dealt with in the same way', and this goes to disclosure of information between different agencies and between different staff who, on the face of it, would have a bona-fide official reason to be handling that information. I just want to check that IGIS doesn't consider there to be any issues because, in paragraph 17, there is 'to ensure there are no barriers, perceived or otherwise'.

**Dr Jessup:** I'm not aware of any reason that those provisions should not be applicable to IGIS, in the same way as exceptions have been dealt with under the Intelligence Services Act, as we've referred to in our submission. I think the short answer to your question is, no, there's no apparent reason. I won't speculate. It is really something that will need to be addressed in the policy space; but it does strike us as being a gap, which perhaps ought to be attended to.

**Senator FAWCETT:** But what I'm getting at is whether you see that gap as potentially presenting problems for your staff and the performance of your function.

**Dr Jessup:** I'd be very surprised if it did in a practical sense. That is to say, you would be very surprised if anyone had in mind the tracking down of staff within the IGIS office and prosecuting them for having discussions about some matter of legality or propriety arising under these new provisions. However, the bill has given its mind to the extent of sharing that is permissible; and, when we were preparing this submission it did stand out to us that this was something that hadn't been addressed.

**Senator FAWCETT:** So, in line with your earlier comments, you are really speaking about the 'avoidance of doubt', which I think is a term commonly used by lawyers.

**Dr Jessup:** I suppose I'm hoist by my own petard in that regard, but that is probably so, yes.

**CHAIR:** Mr Dreyfus.

**Mr DREYFUS:** I think I'll ask both the Ombudsman and IGIS to take these questions on notice because they're somewhat intricate. I'm interested in the views of both of you about detailed suggestions that have been made by the Law Council. Starting at paragraph 284, page 79, of the Law Council's submission, under the heading 'Independent Operational Oversight, it makes a number of quite detailed suggestions about the Ombudsman and the role of the Ombudsman under this legislation, and it makes a number of detailed suggestions about IGIS and the role of IGIS under this legislation. In recommendation 28, which is on page 84, the Law Council makes some quite detailed recommendations for amendment to the scheme, and it continues at page 85 with a specific recommendation about oversight of ASD by IGIS. I would be interested in getting a response. If you want to speak to it now, that would be fine, but it does strike me as being pretty intricate. I'm interested in the views of both of you about those detailed suggestions that have been made by the Law Council. It is up to you whether you want to say something now or take it on notice.

**Dr Jessup:** I think the only thing I would say now is that the passages in the Law Council's submission, starting at paragraph 319, insofar as they relate to my office, are relatively brief. I think my response to the question that you've asked would likewise be very brief, but it would be safer if I took it on notice.

**Mr DREYFUS:** That's fine. There's another specific section of the Law Council's submission at pages 104 to 106 of the Law Council's submission and, again, this goes to notification requirements that my colleague Senator Keneally has asked you about. But given the relative intricacies of the point that the Law Council makes about section 476.6, I think you possibly should respond to that in writing as well, Dr Jessup.

**Dr Jessup:** Yes, I will accept that invitation.

**CHAIR:** We will go back to Senator Keneally.

**Senator KENEALLY:** Just picking up on something that the IGIS submission highlights in relation to ASD, you note that the information gathered by ASD, in the course of exercising its intervention powers, could be used for other aspects of ASD's functions. I found that to be intriguing. Could you provide an example of what type of information you are referring to and how it might be used in support of other ASD functions?

**Dr Jessup:** I think I'm right in saying that the point we were making was that ASD could use that information in relation to the needs of the Department of Home Affairs generally and not just in relation to the Security of Critical Infrastructure Act. Under existing legislation, ASD has specific powers to assist other agencies and bodies. One of the categories of that assistance requires the making of regulations to designate to whom the assistance can be given and, as such, some of the agencies to whom assistance can be given are set out in the act. But there's a catch-all that permits the governing council to make regulations to extend the categories of bodies to whom assistance can be given. So, this isn't a provision of the bill as such, but rather a supporting amendment to regulations made under the Intelligence Services Act, and the new regulations would bring in the Department of Home Affairs as an entity to which assistance could be given. If that is what is intended, we do not wish to enter into the question whether it's a good or bad idea, as that's entirely a matter for the policymakers. However, the point we make is that the explanatory materials—not the explanatory memorandum for this bill but the explanatory materials accompanying the draft regulation that has been released for exposure—suggest that this new prescription in the regulations, which adds in the Department of Home Affairs as a body the ASD can share

information with or provide information to, is for the purpose of the functions of the department under the Security of Critical Infrastructure Act as amended by this bill.

Again, that's fine if that's what is intended. All we're doing is pointing out that the actual regulation or amendment to the regulation does not provide that limitation; it's not confined to the department's purposes under the Security of Critical Infrastructure Act. We make this observation because we have the responsibility to oversee the operations of ASD, so it's important for us to have clarity as to where the line or border over which they shouldn't step is to be drawn. That is the point of our submission. It's a very narrow point, but it's a specific one that affects us from a technical point of view; and, if we hadn't drawn this to the committee's attention, perhaps nobody else would have.

**Senator KENEALLY:** Thank you, Dr Jessup. You've actually started getting into the second part of my question, which is whether these activities by which ASD can provide assistance to Home Affairs would fall outside the SOCI Act. Your reading seems to be that, because the regulation doesn't prescribe or define that assistance, potentially those activities could fall outside the SOCI Act.

**Dr Jessup:** I'm sorry? What was the actual question?

**Senator KENEALLY:** If I understand your evidence correctly, the issue is that the assistance that ASD can provide to Home Affairs is not limited to the activities within the SOCI Act and could be broader than that act.

**Dr Jessup:** It's broader, yes.

**Senator KENEALLY:** It is broader.

**Dr Jessup:** Under the regulations it is broader, yes.

**Senator KENEALLY:** My question was, 'Is it broader?' and you're clearly saying, 'Yes, it is.' Are you recommending that we look at ways to improve that regulation or constrain it to the SOCI Act?

**Dr Jessup:** No, Senator; I wouldn't presume to recommend what you or the committee should do. We're drawing it to your attention, and you might cause it to be drawn to attention through the appropriate channels or in your report, but I certainly would not enter into the area of suggesting what the committee itself should do or how it should approach this issue.

**Senator KENEALLY:** Let me ask it of you this way. If the regulation is left as is and not changed, would that mean that some of the activities by which ASD can provide assistance to Home Affairs would not be oversighted by you?

**Dr Jessup:** No. Whatever ASD does will be oversighted by us, and it's oversighted by us because it's done by ASD.

**Senator KENEALLY:** So, if that regulation were not changed and stayed as it is, what would the implications be?

**Dr Jessup:** It would mean that a broader range of ASD activities would fall within my officers' oversight, but we wouldn't have any problem with that. If the regulation-making policymakers want to give ASD this broader range of functions, we will engage in oversight accordingly. It's just that, in the explanatory memorandum, that regulation appears to have a more limited operation, and our concern is that there might be a disconnect between what the regulation-makers thought they were doing and what they are actually doing.

**CHAIR:** Dr Aly.

**Dr ALY:** I thank the Commonwealth Ombudsman and IGIS for appearing today. I just have one question of IGIS, and it's really for clarification. My understanding is that you currently have oversight of ASD, but this bill would introduce for you, first of all, the ability to share information under a regime with the Commonwealth Ombudsman. The other part that I'm interested in is the new authority of the evidentiary certificates. I wonder if IGIS could please speak to that new authority. Do you currently issue evidentiary certificates in any other respect for any of the other work that you do?

**Dr Jessup:** Yes, there are similar certification-type processes—whether they're certificates, as such, by name or some other similar designation—that IGIS, because of its access to what is happening within the classified space, is able to assist with. Yes, there are similar things. In fact, the Law Council has referred to them at paragraph 197 of its submission. We don't share the perception of the Law Council that they are quite different and do not provide a precedent. In our reading of things they do provide a precedent. But I must say to the committee that, in fact, although those powers under the Intelligence Services Act and the Criminal Code are there, there hasn't been an occasion where we have been called upon to exercise them, and that probably just arises from the fact that they're very unusual things. But we have done other things, such as provide expert evidence under the Freedom of Information Act and the Archives Act; from time to time, IGIS is asked to provide

evidence in those contexts. It's different from the normal oversight thing, but because of the very different functions that we have it's something that we are able to do without any particular discomfort.

**Dr ALY:** You already have the authority to issue certificates; you've just never had to do it.

**Dr Jessup:** Yes, under those other provisions, but not under this bill, of course. This would be a new one. It's not exactly the same. This provision of the bill is analogous; it's similar, but it isn't as though, conceptually speaking, it would be breaking new ground.

**Dr ALY:** The Law Council has pointed this out, but you don't agree with its conclusions in that regard.

**Dr Jessup:** We don't agree with the Law Council's conclusions in that regard. Also, I would be less than frank if I didn't add that we don't agree with almost everything that the Law Council has said in paragraphs 194 to 202 of its submission. I will only go into that space if the committee really wants me to, and it really is mostly a matter for the policymakers. However, insofar as it involves assertions from outside the tent as to what IGIS actually does in intensely practical situations in which its independence might be compromised, such as issues of resource impact and things like that, the committee should not take those paragraphs as representing the position of my office.

**Dr ALY:** Chair, if I may, I want to ask one more question about the framework of what's almost like a dual oversight between the Ombudsman's office and IGIS. Does a current framework exist that you could duplicate for the purposes of this bill or would you have to develop a new framework such purposes?

**Dr Jessup:** I'm not sure what you mean by 'framework'. The two officials—that is, my office and the Ombudsman's office—have oversight responsibilities which, in many ways, are parallel with each other but operate in different spaces. The provisions of the bill and also of another bill before the committee, which is the integrity measures bill, have a capacity for the sharing of information between these two bodies and for a relationship of collaboration, which already exists but will be strengthened as a result of the passing of these pieces of legislation. That is something which, in a day-to-day setting, will be able to deal with questions that might arise as to who does what.

**Dr ALY:** By 'framework', I was referring specifically to the framework that has the shared oversight regime between the Ombudsman and IGIS; it's in attachment B of the explanatory memorandum. I think you have probably answered my question about whether you already have shared oversight with the Commonwealth Ombudsman and, therefore, this being not an entirely new regime for you.

**Dr Jessup:** The short answer is, yes, which is to say, yes, we already have it and, yes, it's not entirely new. A slightly more elaborate answer would draw attention to the fact that both this bill and the expanded jurisdiction that we will have under the integrity measures bill, if it goes through the parliament, will expand the area in which the Ombudsman and ourselves have some point of contact or parallel operations in relation to the same agency. This does seem to be an inescapable circumstance of the fact that, as I mentioned before, IGIS exists because many agencies operate within the classified space that the Ombudsman doesn't have the security clearances to go to. You will always have an area within which IGIS operates, with there being a point outside of which IGIS doesn't operate. But, to an extent, that differential does exist under existing arrangements; it will, though, probably become a more common feature with the new arrangements.

**Dr ALY:** Thank you very much for appearing today and answering my questions.

**CHAIR:** As there are no further questions from committee members, I thank both the Ombudsman and IGIS for their evidence and attendance here today. As usual, you will get a draft transcript to check for any transcription errors that you might like to suggest corrections to. We would be grateful if answers to questions that you've taken on notice could be returned by 4 pm on Friday, 25 June. Also, as some committee members have flagged, you might receive some questions in written form after this hearing. Thank you very much. The committee will now suspend and will return later with the Office of the Victorian Information Commissioner.

**Proceedings suspended from 11:07 to 11:45**

**BLUEMMEL, Mr Sven, Information Commissioner, Office of the Victorian Information Commissioner [by video link]**

**DIXON, Ms Rachel, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner [by video link]**

**CHAIR:** The committee will now resume. I welcome representatives of the Office of the Victorian Information Commissioner.

**Ms Dixon:** Thank you, Chair. As Mr Bluemmel has been delayed, I will make the opening statement on his behalf. Mr Bluemmel and I together hold powers under the Privacy and Data Protection Act. I would like to acknowledge the Wurundjeri people of the Kulin nation as the traditional custodians of the land from which we are speaking today. I would like to pay our respects to their elders.

**CHAIR:** I will come to the opening statement in just a second. There are just a couple more things I need to note. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege.

**Ms Dixon:** Thank you. Can you see me?

**CHAIR:** Yes.

**Ms Dixon:** Thank you. OVIC is the primary regulator for information security, information privacy and freedom of information in Victoria. We administer two acts: the Privacy and Data Protection Act and the Freedom of Information Act. We think we have a fairly unique perspective in promoting fair access to information and in ensuring that it's properly used in privacy and security. In relation to security more generally, we follow a risk based approach to information security, which ensures that government takes care of information and secures it appropriately from misuse and inappropriate disclosure, but also pays the right attention to the right assets.

In Victoria, the PDP Act sets out protected data security requirements for Victorian public sector entities. These requirements cover public sector data and data systems. The act also binds contractors providing services, functions and software to Victorian government agencies, including such disparate businesses as toll road operators and IT service providers. I think this is a crucial point in the application of this act. The PDP Act also highlights law enforcement and crime statistics data security as special cases. Many regulators in Australia do not have this power, but OVIC does have jurisdiction over Victoria Police and Crime Statistics Agency Victoria. The Victorian protective data security model has now been in place for more than four years. It has attracted national and international attention as a very effective approach, grounded in legislation and overseen by an independent responsive regulator with substantial powers and a strong track record. Government agencies, private industry and advisers in the state of Victoria are familiar with the model, as is the protective information security community at the federal level. To this end, our office strongly believes that this established and respected model is seen as a valuable existing tool in protecting critical infrastructure. I would be pleased to answer any questions the committee has.

**CHAIR:** Thanks very much, Ms Dixon. One of the issues raised in your submission is the issue of duplication with existing legislation. This issue has been raised by other submitters, and we had a hearing on a closely related piece of legislation a couple of weeks ago where that was a theme. The Department of Home Affairs has stated that it believes that any duplication will be overcome by the new legislation and that only the higher level of obligations will apply to entities that are regulated by multiple regimes. Is that sufficient to put your mind at ease? Or do you think other amendments are necessary to achieve that?

**Ms Dixon:** I would suggest—and I can see that Sven has joined now—that it's more than the obligation. One of the things we're concerned about is that the duplication will confuse the industry to a certain extent—certainly local government entities that have relationships with commercial partners. We already have the situation in relation to notifiable data breach legislation, where some entities are unsure who they report to. The issue of thresholds can become an issue. For example, the threshold for information breaches under the Commonwealth privacy legislation is slightly different than the one in the PSPF and the business impact table that we use as well. I think the potential for confusion in this space is actually quite great. So it's not a question of which is the more onerous, because fundamentally if you're going for a risk based approach—and I'll come back to this in a second—that's not where the problem lies. Where the problem lies is getting people to make those risk assessments appropriately and understand what those business impact levels mean, how to assess them and whether or not they are actually able to fulfil all those things. It is not a compliance based regime. I think a lot of

the stuff coming out of this bill seems to set minimum standards, if you like. We see a lot of this in the information security community. Its checklist security; it's not security awareness. We have some concerns about that. We work very hard with the community to get them to value their own information because they understand their business.

**CHAIR:** Yes, that's a really interesting point. Of course, we would all want to avoid that box-ticking exercise mentality and want it to be in the interests of organisations to protect the security of their clients, their customers, their suppliers or whatever. If we believe they are not doing that and the legislation is quite a blunt instrument to achieve that, but what other options do we have available to us to ensure we have that level of compliance that is necessary, particularly in critical infrastructure and strategically important services?

**Ms Dixon:** While I won't hold us up to be the ultimate of everything security, I will say that the model that we have in Victoria works in the sense that government do a lot of capability building through, for example, the Department of Premier and Cabinet—that is to say a lot of advising on how to do things. We do the regulatory bit, which is the auditing and making sure that the things that need to be done are done. That's a slightly different approach than is envisaged here. I agree with you that there is a need for a robust framework, but in a risk based framework more attention needs to be paid to the capability than to the stick. When the stick is applied, people generally try to obfuscate to avoid the stick being applied. That's not necessarily a productive way. It becomes security theatre.

**CHAIR:** One thing they can do to avoid the stick is to have the necessary processes and procedures in place to protect themselves and their clients. Isn't that an important motivator?

**Ms Dixon:** I absolutely agree with the question. If I can borrow a line. I believe it was Mike Tyson who said that everybody has a plan until they get punched in the face. What we find is that everybody needs a plan. It's not so much that are you going to get exposed, but what you do when you are exposed, what you do to remediate and how prepared you are and how robust that plan is. Let's just set standards and tell everybody what they have to do because they need to understand where their vulnerabilities are. But then how do we remediate those things?

**Mr Bluemmel:** Just to add to the earlier issue about capability and the limitations of a checklist and a compliance-type approach, one of the things that our system does at the moment is require agencies to notify us of data breaches above a certain relatively low threshold, which is covered in our submission. In terms of the best weapons that we have, the intelligence that we gain from those data breaches is immensely instructive. Rarely is it a case that the system or the process isn't there; it's a case of what is the awareness of all of those individuals along the train. That is why we have invested so much time in building that awareness, getting people to ask the right questions. The best weapon when you have a person on the inside of an organisation that you are trying to protect who has that radar is one who says, 'Hang on, I think we might need to ask a question here.' That is something we have gleaned a lot from that notification scheme that we have.

**Dr ALY:** My first question goes to the scope of this bill compared to your PDP act. One of the things that the bill does is expand the scope of critical infrastructure assets from four sectors to 11 sectors—going from electricity, gas, water and maritime to include other sectors like communications, financial data storage, defence, higher education, food, health, space and transport. Can you comment on the scope of the act that you operate under in terms of the critical infrastructure sectors?

**Mr Bluemmel:** I'm happy to start that off and then I might hand to Deputy Commissioner Dixon. Broadly speaking, our act isn't limited by any of those sorts of things. Our act is really about protective data security in total. But, before we get into more detail, I would say that, as a broad and conceptual comment, the idea that sectors like higher education and so forth are potentially key players in national security—and robustness—I think makes a lot of sense. We are seeing that in the education sector; those sorts of things are often really important in terms of the research, national and international agreements and all of those sorts of things. So, conceptually, drawing that wider boundary is understandable. But, in terms of the PDP Act in Victoria and how that applies to those, I might hand over to Ms Dixon.

**Ms Dixon:** We do have a capacity in our act to write custom standards for particular sectors, if they approach us. We have not issued a customised standard like that yet, but we recently were approached by one particular critical infrastructure sector to help them with some custom standards because they have unique issues with personnel clearances and also with industrial control systems. You won't find the same systems in a telco, for example, that you will find in a water company. That's actually unusual, though. The reason we have shied away from doing a lot of that, again, comes back to the risk analysis. When you think about it, it doesn't really matter which sector an organisation sits in; it's how they manage the risk to all the different components of their operation.

Going further then, the issue is: in each of these sectors, what is so different? What requires a custom standard? How will that custom standard enable them to assess their risks and respond to those risks any better? It also assumes that all of the organisations in that sector are quite similar. A smaller entity may have completely different levels of risk than a very large one with multiple sites et cetera. So we would argue that focusing on that risk analysis negates the need for the complexity of this particular legislation. This one is trying to slice and dice 15 ways from Sunday and provide all of these custom things, such that if you move into a new organisation you have this custom framework that may have been different than the one you had previously—because it's not just IT we are talking about here. As I say, it's personnel security and it's physical security, which is a really important component of securing assets in the national interest space in particular. I think that complexity is the enemy of good understanding.

**Dr ALY:** The act that you operate under, the PDP Act—you only oversee public sector agencies. But you mentioned that any contractors to public sector agencies are also covered by the act. Is that in their contractual arrangements?

**Ms Dixon:** Yes. It has to be. It is part of our act. In the event that they don't, we will come after the head of the agency, the secretary of the agency, and basically hammer them in order to get us access to the companies that have had the issue. I think the first time in my tenure that this became an issue was some years ago with an incident involving a toll road. They believed they were a private company and therefore they were bound by Commonwealth legislation not by state legislation. But, of course, toll roads operate under a state contract. They don't actually own the road. They have the franchise to operate the road. So they're bound by our legislation, and the relevant minister at the time was very keen to stress that they should be abiding by our legislation.

**Dr ALY:** I am interested in the recommendations that you make with regard to the definition of a 'cybersecurity incident'. The one that caught my eye was paragraph 17, where you recommend that the proposed definition in the bill only focus on unauthorised access, but that severe cybersecurity incidents could occur with authorised access—for example, mitigating insider threat or mitigating incidents that weren't deliberate. Are these currently in your act? Does your current act, the PDP Act, have a definition of 'cybersecurity incident' that covers either insider threat or unintentional harm?

**Mr Bluemmel:** Broadly speaking, in terms of the legislation, it doesn't go to that level of detail. It doesn't take it out, for example. It talks about protective data security in general. If we take it back to the general CIA of information security—confidentiality, integrity and availability—anything that is a threat to those is conceptually able to be brought in. Of course, an insider who is using their valid access for an improper purpose who may then harm the confidentiality of the information by misusing it, may harm the availability of the information or the integrity by changing it in an unauthorised way even though they have authorised access to the system and the data in the first place. That would all be covered.

**Dr ALY:** I just have one more question, if I may. With regard to your comments about not having a compliance based regime and that it should be not coercive—if I could use those words. In your experience, have there been examples where the lack of mandatory reporting has actually been an issue?

**Mr Bluemmel:** I think it's probably worth distinguishing that a little. At no point is our argument that there should not be strong enforcement. What we're saying is: 'Enforcement of what?' We are trying to get away from the compliance/checklist approach, where you say: 'Look, I've ticked the boxes. I am secure. I am done here. I can relax now.' That is clearly never a good idea. We want to get away from that and get into the genuine risk management approach, which means that you—and in our case that particularly includes the head of the agency—need to turn your mind to what the risks are. What is my risk posture? What is the value of the information that I collect, use, disclose and manage—and so on? Then you need to find ways to protect that appropriately and to constantly improve that. Either model can still be overseen by a regulator with substantial powers. But that's the distinction we're primarily trying to draw.

**Dr ALY:** Can I just make a point on that. A few years ago I probably would have wholeheartedly agreed with you. But, over the years, I have spoken to a lot of organisations that have critical infrastructure, and I get a sense that there is a heightened awareness of compliance culture, or developing a compliance culture, versus a culture around cybersecurity where there is more of a continuous improvement approach. Firstly, I seek your comment on that. Secondly, would you agree that the awareness that we have at the moment is at an all-time high among organisations that have critical infrastructure—about the need to avoid compliance culture in this space?

**Mr Bluemmel:** Over to you, Rachel.

**Ms Dixon:** The reason we settled on a risk based approach is that essentially the government and organisations generally have a finite amount of money they can spend. This is an infinitely complex field. You

have to choose where to invest your efforts. Obviously that goes to: where are the likely problems in my organisation; what are the things that people are likely to be after; who are the people likely to be after them; or how are they likely to be after them? Bear in mind that I am not just talking about, for example, the theft of information or the ransomwaring of information; we may be, particularly in areas of national interest. If I was a nation-state actor and I wanted to degrade a system by, say, 20 per cent to destroy faith in the Australian government, for example, or in a particular entity, would I be interested in doing that? Yes, I would.

It goes back to that thing of if you have limited amount then spending a gazillion dollars on firewalls and lots of interesting pieces of artificial intelligence to chase bots around a network can be terrific and it can be absolutely appropriate. But if you are doing that whilst, for example, not making sure that your workforce is trusted or that the sheds where you store your critical chemicals or something are not secured, or that your access passes aren't rotated regularly, those sorts of things, then you're doing it wrong. Once you get into the compliance mindset that you have to do all those things then it becomes a mammoth task to standover that checklist. Most people in this space are now focused on: what are the important things that we have to solve, conscious of the fact that there will always be breaches that we did not anticipate? You can't go, 'Great, we've just bought this great software from X. We don't have to worry now.' They are still going to get things going wrong.

The other thing on the compliance aspect—and one of the points we made in our submission which I am still trying to bring up—is that we have had mandatory data breach reporting in Victoria for about 18 months to two years now, since version 2 of our standards were brought in. In all that time, we have never seen an organisation refuse to cooperate with the people trying to remediate. Everybody is eternally grateful. For example, in Victoria we work closely with the DPC cyberteam. They regularly engage contractors that you guys would be familiar with to come in and do remediation work, to go through the logs, to parcel the systems, debug things and get things out of the network. That capability is terrific. I have never come across anybody who has said, 'No, you can't come into our network.' They are pathetically grateful.

This bill allows for the government to basically take over an organisation's systems in order to do that. If I was a shareholder of a publicly listed company that had that as a possibility, I'd be nervous. Do I trust the government better than I trust the private sector contractors to be able to do this? You may get into a situation where you just add another level of complexity where you have government people in the room and the private sector and the private sector's contractors—a whole bunch of people in a circular firing squad. That's not a helpful solution to the problem.

At the early consultation phase for this bill, I actually asked the department, 'Do you have any examples at all of anybody ever refusing assistance?' They were not able to show us any.

**CHAIR:** It's great to hear, Ms Dixon, that you've had such great cooperation from the private sector on this. I'm not sure that has always been the same case at the federal level. I think there are instances where assistance has been declined, and that is of concern. On the question of what value is added by, for example, ASD stepping in to assist a company under attack, do you believe that ASD has unique capabilities that a private sector IT security firm would not have?

**Ms Dixon:** Yes, I do. In prior roles and even in this role, we have had quite a bit of contact with ASD. They are an admirable organisation. They have tremendous capabilities. There is no question about that. They also have an awareness of state actor threats that some private sector organisations would be unable to disclose, even if they did have that information. So I think there is value in ASD being able to work on these sorts of things—as I say, in the same way that we get DPC cyber. I think it is a very powerful instrument. If there is evidence that companies have refused to cooperate, then fine, I will withdraw any objection. We just asked for that evidence because we think that it's a very strong power and that it should be used fairly sparingly, if at all.

**CHAIR:** Yes. I don't think that's an unreasonable perspective at all. It's possibly the case that our agencies are a bit restrained in what they can share in a public consultation process, or even through this committee. We will be asking those questions this afternoon. Senator Fawcett.

**Senator FAWCETT:** I have a question going to the submission by the Information Commissioner. In paragraph 9, you make reference to the existing security frameworks, such as the protective security policy framework, the information security manual, and you essentially make the point that those are existing frameworks, and most stakeholders are familiar with them. Why didn't the legislation seek to build on those instead of making new ones? During the consultation you had with the Commonwealth, did you raise those? Did you get an understanding as to why they felt a new regime was appropriate? Do you have any comments as to why you still believe the existing framework would be a better one to work with?

**Ms Dixon:** In the public consultations sessions that I attended—and I confess that I only attended two of them, although there were many more—we didn't raise it but somebody else did. I think it goes to the fact that everybody is familiar with the PSPF. Even if they have other schemes, like ours, ours aligns very closely with it, for obvious reasons. So people in the information security committee understand how to apply those safeguards. I think that they're wary. But there was no good reason given as to why we needed to move on from that framework. It was just: 'Here is a new thing.'

**Senator FAWCETT:** Okay. We will certainly be asking that question of the department this afternoon. You also talk in the submission about the inclusion of a carve-out to the bill. I'm interested—and for all the reasons that I think you have also verbally stated about overlap, confusion et cetera, amongst stakeholders—the existing 2018 bill envisages there will be overlap to a certain extent with state run infrastructure, state obligations and reporting requirements. Do you have any insight into how well that is working from a Victorian perspective—whether critical infrastructure that is regulated or owned by the state is subject to the 2018 bill?

**Ms Dixon:** No, because I guess we haven't seen a lot—as I say, since our mandatory reporting scheme came in, which was two years or so ago, the incidents that we have seen have been in areas such as health, where unfortunately our act does not apply. Victoria is an unusual jurisdiction in that regard. We have different regulators for the health sector than we do for everything else. When, for example, there were hospital ransomware attacks, we were closely coordinating with DPC cyber in terms of the awareness function, but we were not involved in the response, because we had no jurisdiction there. Beyond that, I'm not aware of other incidents in Victoria involving critical infrastructure that have risen to any level that would require a response from us in that manner.

**Senator FAWCETT:** I'm not so much talking about incidents—but your submission, as I read it, goes to the point of whether overlap could cause confusion amongst stakeholders or duplication of effort. The extant act already has areas of overlap. Are you aware of confusion or unnecessary effort on behalf of critical infrastructure owner-operators in Victoria as a consequence of the existing act?

**Ms Dixon:** The one that would probably be of most interest to us would be, for example, the water authorities, which would fit under those categories. In general, the rule is that they follow ours. I don't think anybody has enforced the Commonwealth piece on them at all. Whereas we have regular dialogue with them, so they are very conscious of our regulation. They have never raised it with us; put it that way.

**Senator FAWCETT:** So when you were calling for a carve-out—the way the submission reads, it essentially says 'carve out Victoria'. Or are you implying that where there are direct and demonstrable overlaps the Victorian approach should stand? Are you envisaging that it would feed into the federal scheme or are you envisaging a complete separation between the rest of Australia and Victoria?

**Ms Dixon:** I'm arguing for a carve-out in the sense that I don't think you can follow two masters. If the Commonwealth scheme were equivalent to our scheme, I think it would meet both obligations. But, as we've talked about previously, if you're going to vary, for example, some of the PSPF controls, which are very, very closely related to ours, then you're going to put two sets of obligations, which may conflict, on entities. It's just going to result in confusion. The last thing this sector needs is more confusion; it needs more clarity.

So we would argue that where an equivalent regime exists—and we would argue that ours is equivalent, although not on the control side of things, not on the 'take over control of the system' side—and that when you follow the same kind of regime in protecting your infrastructure, the obligations should be the ones in the equivalent regime. We would argue that ours is equivalent.

**Mr Bluemmel:** Senator, if I may on that point? There is a model which is somewhat similar: the Commonwealth Privacy Act. It generally regulates the Commonwealth government but also, generally, the private sector across Australia, subject to certain carve-outs. One of those carve-outs is where the private sector entity in question is, for a particular purpose, already bound by a state privacy act. For example, a private sector entity in Victoria operating under a particular state contract is, therefore, governed by the Victorian privacy act. In that case, the wording and operation of the Commonwealth Privacy Act effectively provides that as long as you're following the Victorian privacy act in that regard, you're therefore excused from the obligations of the Commonwealth act. If you're doing other stuff, for a non-Victorian-government client, then, yes, you're back in. It tries to provide a neat join between the two jurisdictions. That, to us, provides a useful illustration of a potential model.

**Senator FAWCETT:** Assuming, when we ask the department this afternoon, they're able to articulate a demonstrably valid reason why this new approach—rather than expanding the PSPF or the ISM—has a reason for being, would you accept the fact that there is then a gap that would need to be closed between your scheme and

the Commonwealth's? Would you be prepared to adapt or modify what you do to fit in with this new framework at a Commonwealth level, to avoid the need for duplication by stakeholders?

**Ms Dixon:** We would certainly look at our framework. We update our framework on a reasonably regular basis; we've had two iterations now, within four years. We try not to do it too often, because we want industry to get familiar with the model. But, certainly, if the Commonwealth came up with new things that we felt would contribute to the security of the Victorian government and its contractors, we would absolutely embrace those. We regularly do. We meet with stakeholders from all of the various jurisdictions to talk about what they're seeing and what they're planning to do in terms of trying to roll out new standards.

I would just make the point that it takes the industry and government several years to get used to a set of standards or a framework for anything, and that good security is better than—there is no perfect security and you need time for it to get better. Any change that's brought in will take a couple of years for everybody to get used to. In the interim, we would prefer an iterative approach rather than a sudden approach, if that makes sense.

**Mr DREYFUS:** I'm conscious of the time, and that we've got our next witness waiting, but I just wanted to quickly raise with you, Ms Dixon, something that you mentioned in your opening statement: your reference to the data breach notification regime of the Commonwealth, which I think you suggested potentially causes confusion for some state agents or state bodies. I wonder, just by way of illustration of the proposition you're putting forward for a carve-out here, if you could outline what are the difficulties in respect of the data breach notification scheme that you mentioned?

**Ms Dixon:** The Commonwealth scheme was designed with privacy in mind. Ours is designed with security and those are not the same thing at all, so the risks to personal privacy are our genesis. When I mentioned that conflict I was not saying this is an impossible problem. As Sven has suggested, we work regularly with the OAIC, for example. But we are keen to understand that the business impact level calculator that we provide, which is linked to the PSPF criteria as well and derives from them, is very clear. It gives very clear circumstances for agencies in which to report. But because it's security based, it means that even when no personal information is exposed with access to systems, it's not personal data that's breached; it might be geophysical data. It might be a whole bunch of other things. It might be financial. There may be no personal information breached whatsoever. Those are the only circumstances where that might be an issue but it comes from the fact that, as I say, we have different parts to our act and one of them is security. Practically speaking for us, it just means a lot of outreach for us to agencies, to let them know that they have these obligations. Where the OAIC is notified first, we take a no-wrong-door approach. If it's been notified to the OAIC, that's better than not notifying at all. We will then log the notification after it's been logged with the OAIC in the first instance.

**Mr DREYFUS:** Has the Department of Home Affairs engaged with your office since you've put in your submission?

**Ms Dixon:** No. The only consultations we have had with the Department of Home Affairs have been at the stakeholder feedback sessions.

**Mr DREYFUS:** Right. So did you raise this carve-out notion with them then?

**Ms Dixon:** We have suggested that they needed to find a way to avoid us tripping over one another, yes. I think in the first meeting that we had, they were unaware that this scheme existed.

**Mr DREYFUS:** We have the Department of Home Affairs coming this afternoon, so we can raise this with them, but I thought I would see what your view of the engagement had been. A final question: How do you see what you proposed working given that not every state or territory in Australia has a regime equivalent to that in Victoria? Maybe the question is: How would this work for entities that have interstate operations or are national as well as operating in Victoria but also have Victorian public service interaction?

**Mr Bluemmel:** If I can take that, what I would suggest there is that, again conceptually, the federal Privacy Act provides a good model for how you define that because, again, it provides that where an entity is already bound by an information privacy regime then that defines the carve-out. For example, if an entity is operating in Western Australia, which doesn't have a privacy act, then the Commonwealth act would still apply. So the carve-out is designed to only be to the extent that the entity is already bound by an equivalent regime in another jurisdiction. That's what I would say; therefore, the carve-out would only apply to those jurisdictions where there is one, like Victoria. In other jurisdictions where that's not the case, there would be no carve-out until such time as that jurisdiction has an appropriate equivalent regime. In terms of the interstate operations, again, that's the same sort of issue that's raised with entities that operate across state boundaries under the Privacy Act. So, again, the way that works is that the Australian privacy jurisdictions that do have privacy laws—obviously they are constantly talking to each other—broadly speaking, they are conceptually equivalent, or conceptually similar, I

should say; therefore, companies may need to be familiar with different regimes. But you don't have the different regimes applying at the same time.

**Mr DREYFUS:** That is helpful, Mr Bluemmel. As I said, we will be taking this up with Home Affairs.

**CHAIR:** We have gone over time, so I hope there are no further questions? I am very grateful for the assistance of the witnesses this afternoon. I ask any questions on notice be returned to the committee by Friday 25 June. You may receive some further written questions on notice. You will also receive a draft transcript in case you would like to make any comments or suggested changes. We are very grateful for your attendance and your evidence today.

**Mr Bluemmel:** Thank you very much, and all the best with your deliberations.

**FALK, Ms Angelene, Commissioner, Office of the Australian Information Commissioner [by videolink]**

**HAMPTON, Mrs Elizabeth, Deputy Commissioner, Office of the Australian Information Commissioner [by videolink]**

[12:30]

**CHAIR:** I welcome representatives of the Office of the Australian Information Commissioner to give evidence at this public hearing today. Although the committee does not require you to give evidence under oath, I should advise you the hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Evidence given today attracts parliamentary privilege. I now invite you to make a brief opening statement before we proceed to questions and discussion.

**Mrs Hampton:** The OAIC is supportive of measures that strengthen the security and resilience of systems, assets and data that are critical to Australia's national interests. A strong cybersecurity posture across the breadth of Australian entities can have positive effects on the protection of personal information. Our regulatory role intersects with the critical infrastructure framework in a number of ways. I would like to make three points to the committee with the goal of building a coordinated and efficient regulatory ecosystem, and eliminating any unintended consequences that the bill might have on either our functions or on the privacy of individuals.

The first point is to ensure the OAIC's functions can continue to operate alongside the critical infrastructure regime. Under the Privacy Act, regulated entities have to report notifiable data breaches to our office. However, there is a concern that the bill will be impede entities' ability to comply with those Privacy Act obligations because the critical infrastructure framework will expand the definition of 'protected information' and prohibit disclosure of this information to our office. The critical infrastructure act already impacts our powers by prohibiting the disclosure of protected information to our office under section 47. The act provides that entities are not required to provide information to any person that has the power to require the answering of questions or the production of documents, and this would include the OAIC when exercising our investigation powers. Item 54B of the bill addresses this issue in relation to its Inspector-General of Intelligence and Security by allowing for the disclosure of protected information where it is for the purposes of giving effect to the IGIS's functions or powers. I submit that this provision should be expanded to cover the Information Commissioner as well.

The second point is about the need for a framework that facilitates an efficient assessment and coordinated response to security incidents by leveraging the combined capability of regulatory expertise. This coordinated approach will deliver a proportionate and targeted response to security incidents. The bill, at item 50, provides for information sharing between the IGIS, the Commonwealth Ombudsman and ASD. This should be expanded to include our office. It is particularly relevant when reporting obligations are enlivened under both the Privacy Act's notifiable data breach framework and the critical infrastructure framework. The bill should also amend section 29 of the Australian Information Commissioner Act to allow our office to engage in coordinated responses.

Our final point is that the exercising of ministerial powers authorised by the bill, such as information-gathering powers, should contain appropriate privacy safeguards. We recommend that, before such powers are exercised, the minister should be required to consider the privacy impacts of those directions insofar as they apply to data which may include the personal information of Australians. In this regard, the bill could be amended to list privacy as a matter the minister must have regard to in determining whether a direction or request is a proportionate response to cybersecurity incident. There is a precedent for this approach in section 180F of the Telecommunications (Interception and Access) Act 1979.

**CHAIR:** Thank you very much for that opening statement, Mrs Hampton. I will ask a couple of initial questions and then offer the call to my colleagues. I'm interested in those recommended amendments you outline in your opening statement. To what extent have you already had discussions with the government about those and, if so, what were their responses to those suggestions?

**Mrs Hampton:** We haven't discussed those recommendations directly with government. We have provided a submission on the exposure draft of the bill, which forms the basis of our engagement.

**CHAIR:** To be clear: you have provided a submission to Home Affairs on the exposure draft. In between the exposure draft and the legislation being introduced to parliament, where any of your recommended changes taken up?

**Mrs Hampton:** No, I don't think so.

**CHAIR:** Have you received any response from Home Affairs about the merits or otherwise of any of your recommended changes?

**Mrs Hampton:** I understand there have been some officer-level discussions since, but I can provide feedback about that on notice if you like.

**CHAIR:** If you could take that on notice, that would be helpful. Mr Dreyfus.

**Mr DREYFUS:** I have a question that relates to something the Law Council has suggested. Have you had an opportunity to look at the submissions? It's a somewhat encyclopaedic submission that we got from the Law Council about this Security of Critical Infrastructure Act. Have you had a chance to look at that?

**Mrs Hampton:** I have.

**Mr DREYFUS:** From paragraph 315 through paragraph 318—this is at pages 84 and 85 of the Law Council's submission, and they follow it up with recommendation 29, which relates to you—they're making a point about the secrecy provisions of the SCI Act purporting to override your compulsory information-gathering powers and they're making a suggestion, really, to bolster your role: that the bill should be amended to provide that the override provision in section 47 of the SCI Act not apply to your information-gathering powers, at least under the Privacy Act. You're welcome to take this on notice, because I would appreciate that, but do you have any comment on it now?

**Mrs Hampton:** Certainly our office is of the view that our information-gathering power should be preserved and not overridden by this act. We had envisaged that the law, as envisaged to apply to the IGIS, might be equally applied to the Information Commissioner such that the regulatory powers available to us under the Privacy Act could continue to be exercised, that we could continue to seek information compulsorily, that the application of the Notifiable Data Breach scheme could continue to have effect, because there would be an exemption from those secrecy provisions for us as there is in relation to the Inspector-General of Intelligence and Security. That was the basis of one of the recommendations that we made in relation to the exposure draft.

**Mr DREYFUS:** Do you think there's been any sufficient explanation as to why this override is being apparently persisted with by the Department of Home Affairs? This is something we're proposing to ask the department about, so don't hold back.

**Mrs Hampton:** No, I don't understand the motivation for that particular provision, but I do think there is an opportunity for our regulatory powers under the Privacy Act to be given fuller effect if bill as it currently stands is amended to include us in the same way as the IGIS is included. This will permit people to continue to comply with those compulsory notices.

**Mr DREYFUS:** Quite a lot of the submissions—and there are a lot of submissions—to this inquiry have raised the potential overlap with the Notifiable Data Breach scheme. Are you able to tell the committee what representations you've had with the private or the public sector about the interactions with the NDB scheme?

**Mrs Hampton:** I don't think that we've had a significant number of interactions with businesses in relation to this particular provision in the bill, but we're very aware of the potential overlap between the NDB scheme and the critical infrastructure regime. There are two potential impacts that are significant, first in relation to the ability of entities to notify our office in the event that they experience a data breach that satisfies the terms of the Medibank scheme where it also meets the criteria for a critical infrastructure disclosure and, secondly, our ability to then compulsorily obtain information relevant to that breach or that entity's APP compliance more generally where there's that overlap. And so that is a concern for us.

In addition to the concerns about being able to gather information about the breach and request information from the APP entities involved, we also think there is an opportunity for there to be a more efficient regulatory response to those breaches if there is a greater amount of information sharing permitted between the OAIC, ASD, IGIS and the Ombudsman's office, all of which may have information in relation to the same set of circumstances and taking potentially divergent regulatory responses. An information-sharing provision in relation to this bill would also be of assistance in ensuring that there's an efficient and coordinated regulatory response at the Commonwealth level.

**Mr DREYFUS:** That's helpful. Thanks very much.

**CHAIR:** Senator Fawcett.

**Senator FAWCETT:** I wanted to know whether the Information Commissioner has any concerns about existing security frameworks such as the Protective Security Policy Framework or *Information security manual* are in certain regards being supplanted or now overlap with the new scheme. Do you think that those other regimes should be a basis for any new scheme? Should they be modified rather than having a new scheme?

**Mrs Hampton:** I think there are a number of different standards that might apply to the appropriate responses to security breaches and security incidents. I would like to take that on notice if that is alright. We haven't considered that as part of our submission, and I'd like to think about that a little bit further.

**Senator FAWCETT:** Sure. In your consultations with Home Affairs around this legislation, was there discussion as to why this new scheme is required when there are these other frameworks in existence?

**Mrs Hampton:** Not to my knowledge.

**Senator FAWCETT:** Thank you very much.

**CHAIR:** We are coming to the end of our allotted time. Do any other committee members have questions? Dr Aly?

**Dr ALY:** I have one question, and that is with regard to the positive security obligations that are contained within the bill and the three aspects of that: the Critical Infrastructure Risk Management Program, mandatory reporting of serious cybersecurity incidents to the ASD and ownership and operational information to the Register of Critical Infrastructure Assets. I wonder if you could comment on that particular provision within the bill and how that fits in with your operations and your obligations.

**Mrs Hampton:** Can I clarify the question? Are you speaking in relation to the Notifiable Data Breach scheme or in relation to the APPs more broadly?

**Dr ALY:** It is to the positive security obligations that the bill introduces, which are the three things: the Infrastructure Risk Management Program, the mandatory reporting and the Register of Critical Infrastructure Assets, which provides ownership and operational information. I'm happy to put this one on notice if you need more opportunity to have a look at it, if that's okay.

**Mrs Hampton:** That would be marvellous. Thank you.

**Dr ALY:** Thank you.

**CHAIR:** If there are no further questions, I thank the Office of the Australian Information Commissioner very much for your attendance and appearance this afternoon. We would be grateful for any questions on notice you received to be returned by Friday 25 June. A draft transcript of the *Hansard* will be provided to you for any comments as well. Thank you very much.

**Proceedings suspended from 12:45 to 13:30**

**BRADSHAW, Ms Abigail, Head, Australian Cyber Security Centre, Australian Signals Directorate**

**FURSE Mr Dale, First Assistant Director-General, Partnerships, Engagement and Programs, Australian Signals Directorate**

**GRUNHARD, Mr Samuel, First Assistant Secretary, Critical Infrastructure Security, Department of Home Affairs**

**HANMORE, Mr Karl, First Assistant Director-General, Cyber Security Services, Australian Signals Directorate**

**HANSFORD, Mr Hamish, First Assistant Secretary, Cyber, Digital and Technology Policy, Department of Home Affairs**

**McGLYNN, Mr Stephen, Acting Deputy Director-General, Corporate and Capability, Australian Signals Directorate**

**NOBLE, Ms Rachel, Director-General, Australian Signals Directorate**

**PEZZULLO, Mr Michael, Secretary, Department of Home Affairs**

**CHAIR:** Welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make a brief opening statement before we proceed to discussion and questions. Is there an opening statement on behalf of both ASD and Home Affairs?

**Mr Pezzullo:** I won't speak for ASD, but Ms Noble has advised, as I understand it, that she doesn't propose to make a statement.

**Ms Noble:** Correct.

**Mr Pezzullo:** I will make one on behalf of the department. I will focus in these remarks, Chair, because I know you want to focus on the particulars of bill to set out some context both in terms of imperative from the point of view of necessity and urgency. Cyberattacks will soon reach global pandemic proportions. This has been building for about five years but has accelerated over the course of the COVID pandemic. The minister has directed that we build on the Cyber Security Strategy launched in 2020 with an increased focus on protecting critical infrastructure—that's what brings us before you today—cybercrime operations, counter-ransomware, along with intensified engagement with states, territories, industry and the general public.

Basic cybersecurity protections will always help, but malicious actors, such as cybercriminals, state sponsored actors and state actors themselves will defeat the best defences that firms, families and individuals can buy. We have to do what we can, of course, to defend our own networks and devices against known vulnerabilities. However, just as we do not rely on home security alarms and door locks to deal with serious and organised crime, we cannot leave firms, families and individuals on the field on their own.

Therefore a regime of critical infrastructure protections is vitally important, but it has to sit within a broader suite which includes enhanced cybersituational awareness and threat-sharing platforms; national cyber exercises, which we are planning to do with states and territories as well as with infrastructure providers; the rollout of the joint cybersecurity centres under the auspices of ASD; threat blocking on our national infrastructure at scale; enhanced cybersecurity awareness, incident response and crisis recovery; securing data through a national data security plan, as well as securing identity through a digital identity plan. I draw particular attention to the government assistance measures contained within this legislation which will allow industry and government over time to build networks securely from the ground up as new IT and OT, or operating technology, infrastructure is built. But obviously we will have to focus initially on legacy networks and infrastructure that support these firms.

We also have to disrupt and degrade malicious actors including through enhanced cybercrime capabilities within the Australian Federal Police, which was recently funded to recruit at least an additional 100 agents to work with ASD in this area. We need new network identification and disruption authorities, and of course there's another bill before this committee—the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020—which will serve that purpose.

ASD will need to lift the tempo of its offensive operations in this area using its authority to disable infrastructure used by malicious actors as well as block their access to stolen information and cryptocurrency. These operations—and the director-general can speak more particularly to these matters, some of which are very

sensitive and classified, and she is the best expert to make that judgement about what to disclose publicly—will need to be carefully targeted and mounted because offensive cyber tools can be repurposed and re-engineered and they can result in blowback.

We have to be prepared to conduct offensive operations in the havens of cybercriminals. Cyber is not immaterial. It is material. It is reliant on infrastructure, hardware, coding spaces for the coders and physical staging points. These havens can be mapped and targeted. Nations such as Australia have an asymmetric advantage because unlike in terms of military strength—where great powers have a symmetric advantage—should we have the will, the strategies, the authorities and the means, we can gain asymmetric advantages including when we go on the offensive. It's already the case that policing and intelligence agencies as well as military cyber forces within authorities are striking at the infrastructure of these malicious actors in their havens, where regrettably some states either turn a blind eye to their activities or actively enable and sponsor them. Regrettably, state protection emboldens these malicious actors.

One model to tackle this challenge is the counterterrorism model that was put in place after 9/11 to deal with al-Qaeda. Another model that I would suggest to this committee, that is worth reflecting on as you consider this bill and consider your report, is the campaign that was mounted in the 17th, 18th and then in the beginning of the 19th century to clear the world's oceans of pirates, including the pirates of the Caribbean who were defeated by Her Majesty's warships of the royal navy in concert with bringing law to a lawless ocean. This is a problem with which we can deal, just as Britain overcame piracy, but we need the tools to do so including the requisite legal authorities. Thank you.

**CHAIR:** Thank you. I will ask a few questions and then I will offer the call to my colleagues. I want to make the most of the time that we have with you today and don't want to waste your time, which is valuable, any more than necessary. A number of the submissions, or at least a number of the recommendations contained within the submissions, are quite technical and go to issues of drafting. Rather than have long discussions about those issues today, I ask that Home Affairs consider either responding in a question on notice or in the form of a supplementary submission to those technical and drafting suggestions that have been made, for example, by the Law Council, the Ombudsman, the IGIS, the information commissioners, and the Western Australian Department of the Premier and Cabinet. We would like to focus on the substantive issues today and the questions of balance, judgement and policy, rather than technical questions.

**Mr Pezzullo:** Chair, we will be delighted to work with the committee in whatever means best support the committee. I have spoken with the minister about the importance of this legislation, and she has made it clear that we are to collaborate, as of course we always would, in whatever ways are in the interest of getting this bill before you to your satisfaction and can support the writing of a report as soon as that can reasonably be done. The urgency and the imperative I have touched on in my opening statement would certainly lend themselves to that kind of assistance. Thank you.

**CHAIR:** Thank you. That's our shared ambition. We don't want to be an obstacle to the quick resolution of this legislation. It would assist us if we can deal with, as promptly and as early as possible, those technical and drafting questions that really aren't material to the balancing questions we face. Moving on to the substantive matters, I will direct this to you, Ms Noble: the secretary in his opening statement has spoken a little bit about the threat environment. I wonder if you could flesh that out a little bit from ASD's perspective and give us a picture, to the extent you can in a public hearing, of how serious the threats that we face are.

**Ms Noble:** Certainly. The threat environment is definitely deteriorating. As evidence of that, there's been a 60 per cent increase in ransomware attacks against Australian entities between this year and last year. One of my US colleagues recently said she thought there was a significant risk of catastrophic cyberattacks in the United States.

My contention is that if you're JBS, Nine or Toll Group—all very brave companies whose representatives have spoken publicly about cyberattacks on their networks—those catastrophes have already happened. The impact of the cyberattacks on their own businesses, on the services they provide to Australians and on the employment of their workers, is in already in the realm of catastrophic.

We see both state based actors and criminals operating against Australian entities. They're motivated by a range of different imperatives, from espionage to generating influence, to interference, to preparing to or actually disrupting, degrading or denying services. Some also have the pure criminal motivation of stealing money; like a lot of criminals, they try to steal it from the most vulnerable using tools that are available on the internet, that are syndicated, that are provided as a service on the dark web and are pretty easily accessible if you have the motivation to access them.

The vast majority of the attacks over the past year that ASD is aware of are focused on critical infrastructure sectors or systems of national significance. For example, we've seen significant targeting of the health sector due to a combination of fragility and a perception that they're vulnerable because their employees work endlessly and tirelessly to help us in a pandemic. Therefore, as a victim, they might be more prone to letting their defences down because they are prioritising other things. They'll then pay a ransom to try to quickly recover. Our data underscores that.

There is also a broader economic cost. AustCyber, for example, have estimated that a significant cyberattack against Australia could cost $30 billion and 160,000 or more jobs. So that's a very quick thumbnail sketch of what we see occurring in our environment.

**CHAIR:** To be clear, to my knowledge most of those examples you cited—whether it's Toll, Nine, JBS or the recent experience in the US with the pipeline—appear to be criminal in nature based on what's available on the public record. But this bill is equally aimed at preventing or safeguarding against state based actors and their motivations in this space, isn't it?

**Ms Noble:** That's absolutely right. In June last year the Prime Minister made a public announcement about one such campaign—probably the most significant campaign against Australian entities by a state based actor. They're out there as well, and it's not only one country; a number of countries have an interest in Australia for espionage, influence and interference purposes.

**CHAIR:** In evidence before the committee today, the Victorian Information Commissioner and the Law Council both characterised the cooperation they observe or that they personally have received from the business community when threats of this nature arise as highly cooperative and very receptive. The Victorian Information Commissioner went as far as to say she was not aware of any examples of where they were non-receptive or non-cooperative.

**Mr Pezzullo:** I should add: and probably too late, because by that stage the house is on fire and burning down. In desperate circumstances people will collaborate. I think, Director-General, sometimes even there you find an obstacle placed in your way.

**CHAIR:** That's exactly what I want to come to, Mr Pezzullo. Has it been ASD's experience that businesses are always as cooperative as they should be when this happens? Because what some of the submitters are trying to understand is why it is necessary to have these quite, some would say, extreme powers to force organisations to cooperate. If it is the case that they are always cooperating, why would it be necessary to force them to do so? Are there any examples where that has not been the case?

**Ms Noble:** Absolutely. That's not our lived experience—we do have some wonderful examples of incredible cooperation. You might recall that in 2019 there was a significant impact of ransomware against the Victorian health system, and that's a good example. We have a close relationship with the Victorian government and they also had a private incident response provider. So this was a terrific example of state government, federal government and private sector working together. 'Good' looks like this: they contacted us so we were able to work with them. They provided us with technical information from their network, like logs and images of discs. That happened on day one. Within 24 hours, we sent incident responders on the ground to work side by side with the Victorian government, the private entity impacted, their private service provider and our staff from the Australian Cyber Security Centre. We were able to fully map the network quickly and to identify the nature of the criminality.

Why does that matter? There's a difference between good and bad, and I'll come back to what 'bad' looks like in a minute. But our value-add there is that our people in ASD are in hand-to-hand combat with criminals and state based actors every single day. We have the benefit of top-secret intelligence provided to us from around the world, not just our own intelligence that we can gather, and 75 years of investment in technical capability to analyse and unpack that intelligence. We have an incredible posture and ability to understand, through our cyberdefence capabilities, what's happening on Australia's internet through, for example, our great partners in our telco sector constantly exchanging threat information with us. So our value-add in that scenario is that our people are much better and quicker at identifying what actors look like and their trade craft. They repeat their patterns—they leave fingerprints. When we can recognise those and have seen them before, we can often act very quickly to remove that malware off the network and get the network back up. With the whole Victorian incident, we were back up and running together in four days. What we left them with was also the tools, training and capability to identify and protect themselves from a similar attack, and to identify it more quickly if it happened again.

**CHAIR:** So that's the good!

**Ms Noble:** That's the good; that's what good looks like.

**CHAIR:** What I'm interested in is the alternative.

**Ms Noble:** Bad looks like this—and this is a real example, but I'm not going to name names, because that's really important. We found out something happened because there were media reports. Then we tried to reach out to the company to clarify if the media reports were true, and they didn't want to talk to us. We kept pushing—sometimes we have to use our own very senior-level contacts; sometimes through people in this building who might know members of boards or chairs of boards—to try to establish trust and build a willingness to cooperate. At times, we have spent nearly a week negotiating with lawyers about us even being able to obtain just the basic information that I described in the first scenario, asking, 'Can we please just have some data from your network; we might be able to help by telling you quickly who it is, what they're doing and what they might do next?'

In this case that I'm referring to, five days later we were still getting very sluggish engagement and were trying to get them to provide data to us and to deploy some of our tools so that we could work out what was By on day 14 were we only able to provide them with generic protection advice, and their network was still down. Three months later they got reinfected and we started again.

That's the sort of scenario where this legislation gives us, through Home Affairs, the authority for more leverage, firstly, to expect these critical infrastructure providers to have better cybersecurity standards in the first place. The best part of this legislation, from my point of view, is that if they look after themselves it doesn't become work for my people. And if their defences are much higher, they're keeping the low-level crims out and then we might be able to focus on the much more sophisticated, highly organised criminal syndicates or state actors. That's where we'd like to focus our energy.

**CHAIR:** That's frankly extraordinary evidence. I presume this was not a small business. I appreciate you can't name them in this context but I assume they fell into the critical infrastructure space. They were a systemically important business.

**Mr Pezzullo:** We can say it was a nationally known case involving a nationally known company that Ms Noble and I are declining to name at this point. Can I add a policy perspective?

**CHAIR:** Please.

**Mr Pezzullo:** We see the Director-General's travails in this area. There's a reason we've gone for these measures, which we contend are proportionate and not oppressive. I was astonished to hear this evidence and you hear it from those who are technically in the game to ensure their products and services are sold and resold and believe they don't need the government at all. And there are others who've got a different perspective.

I don't draw any adverse inferences about their motivations except to say that it's not the lived experience of the agencies, and that's just been evidenced to this committee. But, even if it was, what that evidence suggests to this committee is that there's tremendous cooperation at the scene of the plane crash. Every time one of our planes goes down, of course we collaborate with the investigators and we work out where all the bodies were and the wreckage of the parts and we help with the safety investigation. We would not tolerate what happens on the internet in relation to aviation safety. We learn lessons from crashes but we also regulate the movement of aircraft through our skies.

The development of the internet has been organic and has been driven by a somewhat unusual combination of libertarian impulses on the one hand and profit driven motivations on the other hand. There are lots of good reasons to connect your business to the internet, to connect your plant machinery to the internet, to monitor it—reasons like driving down costs and increasing performance. But every time you connect to the internet you are flying unsafely through air space. We would not tolerate our air space being ungoverned and unregulated by the state. Yes, of course, there are still plane crashes, because you can never reduce risk to zero. But I would contend that the evidence put to this committee is really saying: 'Don't worry about it. Just attend the scene of the plane crash because there's always terrific cooperation.' Well, as you've just heard from Ms Noble, even at the plane crash scene that's not the case. But I would contend that this parliament has got a different duty, which is to think about the regulation of cyberspace in the way you would think about the regulation of other commons.

**CHAIR:** Help me understand why a business would decline the assistance of ASD? Why would they be reluctant to cooperate? I find that very difficult to understand.

**Mr Pezzullo:** Ms Noble, would you like to chance your arm at that?

**Ms Noble:** I will give you my theories. Our lived experience is that once we do get to the point of cooperation we can have more open conversations about this. It can be a range of factors. One response might be: 'No, we're fine. We've got this. We've got a private incident responder and we think we're going to be fine.' That sort of response can be driven by a little bit of ICT professional hubris. 'I want to believe I've got the technical skills and I don't need help.' That's okay. We understand that people feel that way. That's usually before they've fully

appreciated what they're dealing with. Some of these criminals know what they're doing; they do this all day, every day. When you're experiencing that for the first time, it can be confronting. You don't really have the experience to understand what criminals are capable of, let alone state based actors. So I guess there's an element of that. The second motivation—which I think often brings the lawyers into the room and the conversation—is that they haven't had the plans for this occurring. They don't know how they're going to manage their public communications about it. They're concerned about their commercial interests, the people who provide services to them, their brand damage. So there's a—

**CHAIR:** Possible legal liability?

**Mr Pezzullo:** Almost certainly.

**Ms Noble:** Almost certainly. The loss of future business, the loss of their business. They are trying to contend with all of that while they're also trying to contend with the incident and getting the network back up, which is of course their priority.

**CHAIR:** How does holding ASD at bay—about helping fix the problem—protect the organisation from a class action or a prosecution for failing their obligations? It doesn't make intuitive sense. Do they think ASD is going to dob them in?

**Ms Noble:** It's that it's a third party; it's that someone else knows. 'I know you say you're from the federal government and you're not going to talk about what you know publicly, but how can I really trust you? I want you to sign a MOU and a non-disclosure agreement before I even tell you where my network is.' So it can be about trust. But one of the points that this bill goes to is also the fear of, 'If you're in there with us and you give us instructions, who's going to be liable for that, and what will the consequences be?'

**CHAIR:** Yes.

**Ms Noble:** I think this bill will assist in taking away some of those points of concern that create the reluctance to engage with us.

**CHAIR:** Yes, and let's talk about that. Even if the parliament grants you these powers to force compliance, I think this hesitation on the part of the corporate sector needs to be resolved anyway, because we want them to be compliant voluntarily and cooperatively.

**Mr Pezzullo:** Yes.

**CHAIR:** So, what more can be done in the legislation to remove these anxieties that they have? Some submitters have said that the protection from liability that is offered in this bill is not sufficient, that it doesn't extend far enough—for example, that if they are directed to do something by ASD and it doesn't work out well they could be liable for those actions. What can you say to reassure them?

**Mr Pezzullo:** I would emphasise, in evidence to this committee, that we're conscious of that as an issue. And I would urge the committee not to see this as a standalone measure. As I said in my opening remarks, there's a suite of measures. One that I just very briefly touched on—and your question gives rise to an opportunity for me to flesh this out—is that there's a complementary piece of work that was announced last year in the cybersecurity strategy that goes precisely to the question of corporations law, directors' duties and better-practice regulation in this field. It goes back to the air safety and air worthiness example that I just used.

In fairness to the boards and in fairness to the executive management teams that are grappling with this—things like insurance products, the actuarial costing and pricing of the risk, and the depth of the reinsurance pool—the case law is not particularly well formed. We really are in the early days of flight. It's just that the adversaries learnt how to fly and they've got better planes at the moment than most firms. So, my thesis to you would be that, over time, there'll be some corrective actions that are market forming, because, frankly, deeper and better capability will start to be deployed, because they'll have to respond to these obligations. Insurance products will start to be framed, and prudential standards—there's already a prudential standard under APRA's jurisdiction that's applicable. APRA are looking to work with us as part of this better regulatory framework, which is complementary to the obligations.

Just to give the parliament context—and this might be one of those matters to be dealt with by way of supplementary advice—we're not in a position to pre-empt where the Treasurer and the home affairs minister have a joint lead in terms of the comeback on the regulatory environment.

**CHAIR:** Yes.

**Mr Pezzullo:** We might seek their guidance as to how much we can put forward. Addressing some of those questions of liabilities is, we would contend, best not dealt with through this legislation but through complementary mechanisms that might go, for instance, sector by sector. It might be dealt with through

corporations law, for instance, if it goes to duties. There might be some challenges and issues that the Treasury needs to work through in terms cyber insurance and reinsurance. We would contend that this parliament is faced with a multidimensional challenge that's going to require a series of tools that are interdependent. If we wait for the full suite of tools to be laid out, we could be waiting for a year, two years or three years. This problem is growing exponentially.

Those are live issues; they're important. We would contend that the obligations that are laid out in the bill are proportionate and the immunities are reasonable for the direct actions that Ms Noble referred to. Mr Hansford might want to flesh out the protections and immunities of, in effect, the firefighter running into the building to deal with the fire, which is the point at which ASD's really involved, in the most egregious cases. But I do want to draw the committee's attention to parallel and consequential work going on in the regulatory space that is coming back to the government at the end of the year. Mr Hansford, do you want to add anything on the immunities question?

**Mr Hansford:** I would maybe make just two points. The first point, and to pick up on some of the director-general's evidence, is that a company has to be unwilling or unable for the action directions and for some of the measures in the ministerial authorisation. In the circumstance in which some of the legal issues arise, such as a contractual issue that a firm is worried about, you could effectively issue a friendly notice where a company is unable, because of a commercial litigation issue or a commercial contractual obligation, to work with the government. So I think it can actually be used on the flip side as well to work with the government and protect them in a certain way. On the question of other things in the bill that help, if you look at the concept of the system of national significance and the enhanced cybersecurity obligation, that provides a whole range of other mechanisms to help with companies. For instance, there may be requirements to have an incident response plan; undertake cybersecurity exercises, which the secretary also covered in his opening statement; undertake a vulnerability assessment; periodically report system information; and undertake potential installation of software to provide telemetry. I think these are elements which raise the capability of companies, particularly of those assets that are particularly sensitive. The whole regime, hopefully, over time, will uplift capability. So I think that the immunity sits within a broader context as well.

**Mr Pezzullo:** Can we also address the question of liability—questions that directly arise from ASD's actions—because I think that was part of the chair's question.

**Mr Hansford:** Sure. In the bill, the liabilities we've put in place relate to the action directions that the technical assistor would undertake with a company. If something were to go wrong in the exercise of an action or a direction, the liability then applies. You might think of an example about working to rectify a cybersecurity incident in which you reset a software system, which might cause an outage. The liability from the people who are helping with the asset and the asset provider themselves to try and respond to that incident is a scenario that we've considered in which the liability extends to rectifying the cybersecurity incident. We'd say that the liability is also acting with direct proportionality to the threshold by which they have to be deployed. So there has to be a cybersecurity incident that's about to happen or has happened, and so that's hurdle No. 1. Then there's having ministerial authorisation. The powers are designed to rectify the cybersecurity incident, and it's all around the rectification of the incident. It's not broad-sweeping liability for any action; it is purely in relation to the high thresholds that are in the legislation, the extent of the action that's been approved at ministerial level and then administered by the secretary, and the impact on the business. The extent to which that liability then extends right down to customers, I think, is what some individuals in their evidence before the committee have a problem with.

**CHAIR:** One final question from me, and then I'm going to offer the call to Senator Keneally next. One of asks of this committee is to recommend that there be some sort of an appeal mechanism to contest the step-in and direction powers. Is there a way in which that could be done without harming the capability, or are these powers envisaged to be used in such extreme circumstances that litigating at that point is going to be too costly?

**Mr Pezzullo:** All administrative decisions taken under statutory schemes, intrinsically, of course, are reviewable in terms of administrative decision through judicial review. I think some of the submitters, Mr Hansford, have either called for such a mechanism or, in some cases, even postulated an appeal process. We would contend that the way in which the obligations are laid down by the minister at the authorisation level and then through rules that flow from those authorisations that the secretary then imposes has to be proportionate and tied back to the nexus that's set out in the legislation. You can always litigate, because it's available in our legal system to seek both administrative relief at merits and also judicial review. But let's think that through. We're focused thus far on incidents: pipelines are being frozen, meatworks are being stalled and food processing has been stalled. I think there would theoretically be little prospect that the director-general or I would be called into a case in the Federal Court. From what I've read of the submissions, the concern more is for the proactive measures

where there's no incident. It goes to the aviation safety model. You're trying to lift the safety regime, so you've got to have a risk plan and you've got to have an incident response plan, which you've got to submit to annually to me as the secretary so that I can have it checked by the DG. Mr Hansford, just assist me here: it would be open to anyone to go to either the AAT or the Federal Court in those instances, but—

**CHAIR:** My understanding is that the anxiety is more around these kinds of emergency scenarios—

**Mr Pezzullo:** Yes.

**CHAIR:** As has been articulated to me by some companies, ASD is going to come in and trample around their sensitive systems in a way that they don't agree with, and they've got no ability to say: 'No, don't do that. Please do it this way.' They have no ability to negotiate it or—

**Mr Pezzullo:** We'll look at the detailed proposals and come back to you through that supplementary mechanism that you suggested at the start, but—and the director-general can speak to the calibre of her staff—to that we would say: 'Yes, you might know your system better. But the fire brigade know the attacker better.' There's conceit and hubris that you sometimes get in these discussions, and I've seen it, because Ms Noble has also enabled the assistance of cabinet ministers, secretaries and all sorts of folks. Typically, the CEO or the board member says: 'I've spoken to my CIO. It's all in hand.' Yes, they understand their architecture. Through mergers and acquisition, they actually don't know where their data is scored. They don't know where their cloud provider is. ASD is there with the fire truck, ready to start pumping the water, and they say: 'We know who's causing it. We can break the attack. Do you really not want us to help?' So in emergency situations it's theoretically possible, I suppose, that we'd find ourselves in the Federal Court, but that company's reputation, I would suggest to you, after we've taken a decision to intervene in a way that's proportionate to the threat, would be trashed through the legal proceeding, because we would have to lay in evidence, because of the nature of the plaintiff's case, just how poor their cyberdefence was and the lack of awareness that they had of the nature of the attacker—that is, where the attacker was—and their shareholders would be confronted with a situation where they'd say, 'You had the world's best fire brigade, and you didn't ask them to put out the fire.'

**CHAIR:** What I'm more concerned about, though, is time lost and the damage done in the meantime if these issues are being litigated.

**Mr Pezzullo:** In an emergency legislation, is there anything particular to the statute—just remind me, Mr Hansford—that specifies the type of judicial review, or is it just simply general judicial review in play?

**Mr Hansford:** General. We've covered the ADJR within the government assistance measures, but we have included consultation at every stage, short of a peak emergency where the government can utilise some national security intelligence to then step in and rectify an issue. There is consultation built in, there are information-gathering powers prior to an action direction, and there are consultation requirements prior to the top level intervention power; there's consultation at every stage short of a peak emergency. Equally in the design of the first part of the legislation, which I note that you weren't so concerned about, there are 28 days of consultation for all of the rules, and that's to be available—

**Mr Pezzullo:** Outside of an emergency.

**Mr Hansford:** Yes.

**Mr Pezzullo:** So, assuming outside of an emergency through the consultative process, if you get to the end of the 28 days and there's still a difference of view, I suppose, theoretically, even there, you've got a merits and judicial review. If the point of your question relates to a crisis, we'd have to say, 'See you in court.' But the law requires the Minister for Home Affairs to make a decision—in effect, tasking ASD, with the agreement of the defence minister and the Prime Minister. We would not put them in a position where we'd say: 'I'm not really sure about this. We don't really think that this dramatic intervention is required.' We would almost certainly have the threat information, the intelligence on the attacker, the gravity of the attack and what they're likely to do in follow-on. You saw the pipeline and you saw the meatworks. If a company really wants to have that in court, I would regrettably have to say: 'Of course, they've got a right to. But it would be foolish in the extreme.'

**CHAIR:** Ms Noble, is there anything you wanted to add on that?

**Ms Noble:** I do want to add the pragmatic reality of what actually happens when we go in to help a company. My colleagues might want to add to this story. The reality of it is that we'll bring our weapons to bear—our intelligence, our deep knowledge of what these actors look like, our ability to reverse-engineer malware and our ability to reach back to Five Eyes partners—but we can't go in there alone and not operate in a collaborative way with a network owner anyway, because the things that we need them to tell us are: Where is your network? How do you pull the logs off? Who's your incident responder? It's not unusual for them to say, 'They're in India,' or are

very far overseas. We'll say: 'Okay, we can't get them here. Where is your incident response plan? What have you normally done?'

The reality is that, when we're working well with a company and we're working well in the spirit of our national interest, because we're talking about organisations whose services or capabilities are providing a service to the nation—they're part of our critical infrastructure; they're not any small company—on the day, we have to do this in partnership together. We will listen and hear their expertise about their network and what we hope, in exchange, is that they will listen and hear and act on our expertise about how to fight criminals and state actors who have malign intent. That's the reality of what it looks like on the ground.

To the extent that those national interests then intersect with their own commercial interests, because their priority is to get their network back up for the customers, their service and the people that they employ, that's the reality of how these things work now. It happens now. We do this with companies when they let us in voluntarily and want to act in those joint and shared interests for the nation. What this legislation does is provide safety nets, imperatives and expectations for those corporations who don't choose to act like that, and time is the imperative here. In a scenario where we're in a court and the power's out in New South Wales—

**Mr Pezzullo:** Yes, good luck with that. Mr Chair, I know that you want to move to Senator Keneally, but I have one very brief comment on the virtuous cycle of doing the proactive work outside of a crisis—the lodgement of incident response plans, the lodgement of a cyber-risk plan, the flow of information that will come into the home affairs department, to our regulatory area, which we of course then share with ASD. Over time ASD, I anticipate, Ms Noble, would build a catalogue of war plans, for want of a better word, or game plans, to say that this sector is configured like this, whereas that sector uses Cloud or something similar. So, their emergency response is actually enriched and improved by working collaboratively outside of a crisis. The proactive, if you will, peacetime operation of this statute helps in the crisis times as well.

**CHAIR:** Thank you very much. I've taken up enough time. Senator Keneally, thanks for your patience.

**Senator KENEALLY:** Thank you, Chair. Thank you to the department and to ASD for appearing today. I might just pick up on this point about contestability, if we can use it in those terms, or an appeal mechanism. Some submitters, particularly those representing sectors or industries that are impacted by the legislation, have suggested that, where there is a dispute about the appropriate mitigation to a cyberincident, the act might be improved by providing for a competent, independent assessor to determine within 12 hours whether an alternative solution put forward by the critical-infrastructure owner or operator is a more appropriate mitigation. The suggestion is that this could be modelled after the provisions in the TOLA Act. Does the department have a response to that proposal?

**Mr Pezzullo:** We do. Of course, I won't speak for how the government might respond to any proposition from this committee along those lines; I'll just venture a view which is within the logic of our current position. Obviously, should the committee see fit to at least recommend to government that it be considered, I don't want to rule out the freedom of action for future government consideration, save to say that, unlike the TOLA position, where there are questions of liberty, they're quite specific—and you saw a use of the TOLA power just the other day with the Ironside computer access warrant—they're quite targeted measures that relate to devices and networks, typically to gain intelligence or to build evidence in relation to a criminal activity or a terrorist activity and the like. For entirely good reasons, the parliament has granted us those powers, with built-in mechanisms for dispute resolution or at least advocacy by appointed officers.

I would contend, Senator, in response to your asking me what the department's view about that might be, especially in the sort of scenario that would require a 12-hour turnaround, that 12 hours might be the difference between a lot of people dying and not many people dying or no people dying at all—the knocking out of a hospital network, the knocking out of a power grid, the knocking out of traffic management systems and the like.

**Senator KENEALLY:** I appreciate the argument you're putting. Nonetheless, in that context, your point about good luck in trying to go to court while the lights are out—the provider—it's even to provide the avenue, because in the scenario you're putting the difference could be five minutes. Quite frankly, it could be a few moments. It would mean that there is no capacity whatsoever for the operator to actually negotiate or respond to a request or direction.

**Mr Pezzullo:** Yes. This goes back to that virtuous cycle that I was addressing towards the end of Senator Paterson's line of questions. Our preference is that a government assistance measure—and this is where the fire brigade metaphor is entirely apposite—isn't just about a measure taken during a crisis. As the other obligations are acquitted in terms of reporting on risk management plans, cyberplans and the like, the government of the day—the Minister for Home Affairs, consulting, as she would be required to, with the Prime Minister and the defence

minister—might proactively direct a company to accept, for instance, ASD capabilities on networks, outside a crisis, that would have a response time in milliseconds. That is to say, for example, that they could kill an attack that was potentially going to infect the whole electricity grid. Forget about 12 hours; we're talking about a millisecond detection/response/block and, potentially, retaliation.

In that context there's no suggestion of doing that in a crisis. I would accept, in response to your question, that having a sensor package—and Ms Noble can better describe her tools in a public forum than I will venture to—let's say, generically, a sensor and response package, from the Australian Signals Directorate, would certainly be a very high-end use of this legislation. However, before you got there, all of the consultative codesign arrangements and involvement by ASD in the codesign process with Home Affairs would have got us to the position where, literally, not just the best cybersecurity experts in the world, some of whom are sitting to my right, but the best intelligence-collection experts in the world would be there. This is where the gap is: no company will ever have a view of the threat as good as that of the ASD, the NSA, GCHQ and other colleagues.

To think that a CIO or the technical adviser to a board or the CIO would have a better view, not just of the mitigation but of the threat, is not plausible to us. We know this industry very well, and we know what we do and can do both in classified collection as well as offensive operations against the targets. I won't speak for 'we' in terms of the government. My view, as the secretary of this department, is that an independent assessor is like a third party between two very deep experts. The company is an expert in its own system, networks and devices, and ASD is an expert in what they're experts in. We contend that the blending of that expertise through synergistic collaboration through the codesign process should get you to a point where the optimal solution, both in relation to the network and to dealing with the threat, is arrived at. I just don't see, personally, what value a third party would add in that circumstance.

**Senator KENEALLY:** Can I push back a little and say that, clearly, there are some business sectors, or some of the sectors which are going to be covered by this act, who don't feel confidence in that synergistic expertise coming together. That's because they're the ones putting this proposal forward.

**Mr Pezzullo:** Yes.

**Senator KENEALLY:** With the greatest of respect, we have to take that view they're putting to us seriously, because they're the most directly affected.

**Mr Pezzullo:** Understood.

**Senator KENEALLY:** I understand the point you were making about people dying, and no-one dismisses that. But this bill goes much further than the 2018 version of the bill. It brings in a range of sectors where, with the greatest of respect, people are unlikely to be dying. There may be a significant impost, whether we're talking about food or petrol delivery. But not every risk within this sector is the same, so it's quite understandable that some of these sectors have raised concerns with this committee about whether or not they should be able to have access. They're thinking about their own systems, their own shareholders, their own business. I'm wondering if there is not some separation in terms of whether we are talking about a true piece of critical infrastructure as was defined in 2018 and some of the other sectors that appropriately have been dragged into this regime.

**Mr Pezzullo:** I might give Mr Hansford some license to venture a view. I know committees are not meant to call for opinions, but I wish to license Mr Hansford such that he doesn't feel he is speaking for future government action. Obviously we will take the report of the committee and provide advice to the government at the time. Mr Hansford, what's your view on the value that would be added by some sort of third-party advocate or mediator or monitor or adjudicator?

**Mr Hansford:** I think it stands in direct contrast to the position in TOLA, which is about, in the circumstances, the development of a technical capability notice, which is effectively done in slower time. The way this bill is being designed is to respond quickly but proportionately to an incident, which is in stark contrast to a capability. That's the first point. The second point is that the Minister for Home Affairs must not grant a ministerial authorisation unless a range of elements are satisfied. They include: that the response would not amount to a practical and effective response to the incident, which then narrows the response; that the entity is unable or unwilling to respond to the incident; that they can't take all reasonable steps themselves; that it is reasonably necessary; that it is proportionate; and that they comply with the specified request and that that is technically feasible based on the advice, principally, from the regulator but also the Australian Signals Directorate. Some of the advice may not be available to the asset and be unique to a particular national security event. Only then, once the Minister for Home Affairs and the Prime Minister and the defence minister—we'd contend that they are the elements which provide a check against the wanton use of the power. They are very specific, very proportionate, necessary and rely on technical feasibility to respond to an incident. In that

circumstance, we think adding an additional layer of a technical adviser—noting the fact that we have been required in the legislation to have consultation with the asset provider—might not be warranted in the event of a cyber-incident.

**Mr Pezzullo:** Can we narrow it, Mr Hansford, to the point the senator raises in relation to what the submitters have been saying. Everyone is on the same page in terms of goodwill and best will. If the company, which knows its system—and it goes to Ms Noble's earlier point—better than ASD but ASD knows the attacker, and there is a genuine good faith difference of view—I'm asking you to play devil's advocate to support me in giving this evidence—would there be a narrower role within those parameters for an independent third party to provide the minister, or someone else, with some sort of technical view about any difference of view about the measures that might work best on the company's network? The company is often the best expert on its own network so, in a more narrow sense, would there be value in a third party?

**CHAIR:** I might have to ask you to join the committee, Mr Pezzullo—this questioning expertise!

**Mr Pezzullo:** I'm trying to get it clear in my head because the senator has asked me—and Mr Hansford understands the legislation.

**CHAIR:** It is generally helpful. I'm being facetious.

**Mr Pezzullo:** Thank you.

**Mr Hansford:** Legislatively it is definitely possible. But the director-general might have comments on technical feasibility and the types of people available.

**Ms Noble:** We would like to venture a view on imagining who that person would be and what that would be like in reality. I'm going to ask Ms Bradshaw to speak to that.

**Ms Bradshaw:** As we have worked through the legislation and operationalising it, the first thing I would say is that the actual threshold for these types of directions is high in the first instance. They anticipate, by definition, a significant impact. Secondly, we would envisage that the making of such a direction or action or request would be done in conjunction with ASD, which is already working with the entity, on the basis that we understand a range of options that are available and the potential impacts. As to the notion that we would draw up or invite a course of action—which, in an operational sense, is more likely to be, 'Please run this script,' or, 'Run this patch'—without a cognisance of the impact or without having had a discussion with the business about their ideas on options or variants, that is not the way that we would see operationalising this piece of legislation. Thirdly, it is very difficult for me to envisage who that third party might be that could operate in an explicit 12-hour framework with an instant understanding of complex OT networks, let alone a contemporaneous understanding of the TS, or top secret, environment. Lastly, my learned operational experience is that time is always of the essence. While 12 hours might sound like a short amount of time, the best proposition about this legislation is that it reduces the time between action and incident. Early access to the fact that there's been a vulnerability prosecuted, that there have been indicators of compromise, means that we can assist to stop lateral movement, we can assist to close down vulnerabilities, we can warn others and we can minimise harm. Very importantly, it gives us the broadest range of options to actually stop further harm, including through the use of effects and offensive operations. Asking ASD to use its unique capabilities to stop malicious cyberactivity without that access to networks or information is like asking the police to catch a burglar without access to the house and without an understanding of which window they got in through. We need all the technical artefacts that lead us to the fullest range of effective response options.

**Senator KENEALLY:** I don't mean to interrupt you, but we will have limited time today and I'm sure that my colleagues have questions as well. I think I've gotten the view from the department and ASD, and I appreciate that. I do have other questions, some which relate to this and some which go on to other things. One of the other requests that have been made of this committee in some of the submissions is about the requirement to notify of a cybersecurity incident that would have a significant impact on the availability of an asset. Some submitters have maintained that to do that within 12 hours is, firstly, unrealistic—they say it would take some time to work out if something is a cybersecurity incident or something else that is happening—and, secondly, it seems to be in contradiction with comparable domestic regimes such as those managed by APRA, which require reports to be made within 72 hours. I anticipate you're going to have a similar answer, but I just put to you that some of the submitters have argued that they should have 72 hours to notify or, perhaps, 12 hours to notify and 72 hours to offer a proposed way forward. Has the department considered the fact that it may well be contradictory to other notification regimes, like those of APRA, and, secondly, have you considered some kind of modified system whereby you tell us something is happening and then, within a certain time frame, you tell us what you think should be done about it?

**Mr Pezzullo:** I'll ask Mr Hansford to speak to the provision, which is either in the Banking Act—

**Senator KENEALLY:** Yes, the Banking Act.

**Mr Pezzullo:** or in any subordinate instrument that APRA manages. I'll just make a comment on the question of whether this should feature in primary legislation or whether it should be part of the apparatus of rules, obligations and reporting obligations, and the point about not even knowing if it's a cyberattack. We saw the other night a massive internet outage, and it was thought initially it could be a cyberattack. It ended up being one of the data provider companies that sit just below the internet having an outage. We would contend, even in that circumstance, it's better to report it early so that Ms Bradshaw and her people can start to think about it. Is there a pattern emerging? Do we know something on the classified side that tells us that this is actually an attack, whereas the company might think that it's just an outage? Whether that is a preliminary form of notification that could be followed up with more evidenced or thought-through detailed notifications, I would contend to you and the committee that it's better to put that into the rules rather than make it a requirement in the primary legislation. It gets so fixed in place once it's in the primary leg. Obviously, it's up to the parliament as to how it chooses to configure the powers. We think that could be just simply to create a filtering and triaging process for the Australian Cyber Security Centre to have some kind of preliminary reporting regime that says: 'Something's happening on our network. We don't know what it is. It might be that a Homer Simpson has decoupled the cable. It might be an outage caused by a provider, or it could be a cyberattack.' It might well be that Ms Bradshaw, who works within the ASD and is also a deputy director-general of ASD, is seeing other intelligence on the signals side that says, 'No, we know what that is.' Now—

**Senator KENEALLY:** Actually, can I just stop you right there before Ms Bradshaw speaks? The other issue that has been raised with us is what appears to be a lack of notification from ASD to a sector, a company or an operator of infrastructure when ASD sees something that's happening. You just mentioned the ASD will know whether this is a cyberattack: yes, it is; no, it's not. Is there, within this regime, a requirement for ASD to notify operators?

**Mr Pezzullo:** We would contend that the measures that were first laid down in the 2016 Cyber Security Strategy but significantly enhanced in the 2020 version are for a threat-sharing platform, which is a government initiative. We are building a threat-sharing platform to enable the director-general and her officers to monitor threats—and I'll get Ms Noble and Ms Bradshaw to speak to the threat sharing—and we would contend that that doesn't need to be mandated in law. I understand the submitters saying there's a tennis volley going on here. We're the government and we are here to help, so we want to share the information. We often need to figure out how to redact it when it's from highly classified sources. I'll ask the director-general and her officers to speak to the threat-sharing obligation the government has imposed on itself through the Cyber Security Strategy 2020. We're looking to significantly interface that with other portals that relate to threat and sector information sharing that the department runs through the Critical Infrastructure Centre, which is also within the department. Before we jump to that, can we get Mr Hansford to clarify or address himself to the question of the Banking Act?

**Mr Hansford:** I think the very first point of the 12 hours is to start a conversation, and so in the 12-hour threshold you've got to fulfil the legislative requirements. Effectively, the clock doesn't start when something happens; it's when you become aware that you have an incident and it falls within the category. The more detailed information about the content of the notification will fall in the rules, which will be subject to co-design. But the first notification can be oral and then subsequently, within 48 hours, it must be given in written form. That's for the 12-hour period. It's a completely different regime from APRA's regime because this is about critical cybersecurity incidents within the 12-hour block. Following consultation with the private sector and particularly with people who are subject to the banking regulations and APRA's legislative regulatory remit, we did align the 72 hours within this bill with APRA's about the other cybersecurity incidents which impact the availability, integrity, reliability or confidentiality of the assets. We have tried to align in one way, but for particularly critical cybersecurity incidents we've put 12 hours. As I said, there is an oral notification.

**Mr Pezzullo:** In terms of threat sharing, I might pass to the director-general.

**Ms Noble:** The Australian Signals Directorate does, and will, always reach out to any Australian entity if we think that they are the subject of a cyberattack. We do that day in, day out. We have a 24/7 operation centre for that purpose.

The second part of this story is that quite a number of employees of the higher-end critical-infrastructure-provider systems of national significance owners that we're talking about in the context of this bill are starting to embed their people with us at the Australian Cyber Security Centre. They're very welcome to do that. We sponsor their clearances and we have physical space for them. We give them access to our intelligence, our networks, our tools and our capability, and we're embarking on this in a genuine partnership to protect our country.

The Australian Cyber Security Centre is a whole-of-nation standing task force that's been there since at least 2018. We have ASD, law enforcement, AFP, ACIC, international partners and Australian private sector companies all working side by side. To supplement that we have threat-sharing platforms, and I'll hand over to Ms Bradshaw to explain how we're trying to build those with the money the government gave us from the Australian Cyber Security Strategy 2020: $1. 35 billion to be able to share the threat information in real time at machine speed.

**Senator KENEALLY:** If I may—and, again, I'm not trying to cut you off, it's more a sense of there being such limited time this afternoon. My question went more to what appears to be from the submitters, not a shared confidence that that's what's happening. Maybe it's a lack of awareness on their part, maybe it's because they're newly brought into this regime or maybe it's because they feel like the bill puts all the obligation on them and no obligation on the government. So it's more of a philosophical point in some ways, and also a point about gaining public confidence.

You've given me some useful information and I'm happy to take any other information on notice. I'm really keen to share the call and not hog all the time, but I have a range of things to get through. One of the other submitters raised with us questions about whether the step-in powers in directions might relate to things that are not IT related, so to speak—if I can use layperson's language there. For example: in a circumstance where there might be a ransomware payment demanded and the government might, for one reason or another, have a view about whether a ransom should or should not be paid—for police investigation purposes or whatever reason. Could you clarify for people who might be watching whether that's also part of the powers that would be available to the minister under the step-in powers?

**Mr Pezzullo:** Yes, insofar as I'm going to interpret 'step-in powers' to mean a particular thing. It's not necessarily under the government assistance measures, or GAMS, as the acronym goes, but, potentially, before you get to that point under a positive security obligation, which might be either physical or virtual. It has to be remembered that our focus has been very much on cybersecurity, and that is certainly the topic of the day. But the act will also give the minister the power, in a way that of course has to be consistent with other legislation, to impose requirements in the physical world, including things like access control, employment security identification procedures, cards and processes. It could relate to the physical protection of a port, for instance, or a piece of physical infrastructure. So, yes, it relates beyond IT and OT at the level of what are known as the PSOs—the positive security obligations.

The second tier of measures are all intrinsically cyber. They're enhanced cybersecurity obligations, so, obviously, they relate to IT and OT. As I heard your question, it might relate to questions of policy and, if you will, programs of activities that aren't strictly in themselves IT. For instance: with the payment of ransom, you're right. In those circumstances—and this happens with law enforcement generally—the government would lay down broad policy and, in some cases, they might seek to legislate. I touched on a ransomware strategy that we're working on to counter ransomware. The government would come to a policy disposition, for instance, on mandatory reporting of ransomware attacks, and that may be a position that may or may not involve prohibition or criminalisation. I don't want to give rise to any speculation that that's where the government will land. If the policy was set in the particular way, so we roll out, pursuant to the cybersecurity strategy from last year, a ransomware strategy, elements of it would attach themselves to PSOs, enhanced cybersecurity obligations and government assistance measures or would potentially relate to other legislation such as the bill currently before you on identifying and disrupting networks. It's really a question of where the best legal authority is to give effect to the measure, not all of which, as you rightly say, will be a strictly IT related measure.

**Senator KENEALLY:** Are you saying that this bill would give latitude for directions to entities, for example, to do something in the physical world?

**Mr Pezzullo:** Yes.

**Senator KENEALLY:** What kind of indemnity is available to companies or operators in those circumstances? You talked about the indemnities, in terms of ASD and their technical interference, so to speak, but what about indemnities that might flow in the physical world?

**Mr Pezzullo:** The same principles that Mr Hansford laid out earlier in relation to both liability and immunities for the actors. Clearly it's a different kind of liability. It's not as though, outside of IT, where ASD might well be directed by the home affairs minister to come onto a system—and we've dealt with the question of the proportionality, the care, the co-design and, as Ms Bradshaw spoke about, the need for the company and ASD to work together. But, in the physical world, I suppose it's no different from the government regulating things like transport security or requiring aviation security identification cards or MSIC cards: it becomes an obligation that

this parliament decrees. They're not just powers that are graced, if you will, to the minister or the secretary or the department; they're obligations that the parliament indicates are required to be met by all sectors of society.

**Senator KENEALLY:** That's not what I'm asking. Say company X becomes the victim of a ransomware attack. They want to pay because they don't want their information dumped in the public realm. The government says: 'Don't pay. We think we know who it is. We're about to get them. Hold off paying.' I'm just making up a scenario. In that circumstance, if the company doesn't pay and their information gets dumped out, they'll say: 'Hey, government, you've really stuffed up. Now we're in a world of pain.' That's a scenario that was put to me by stakeholders, and I'm trying to understand, from you, whether this act allows for that type of scenario to take place, and, if it did take place, what indemnities would be available.

**Mr Pezzullo:** I'll just consult with Mr Hansford. Without being too hypothetical, but equally we need to deal with scenarios—and given we are working on a targeted ransomware strategy that will deal with the question of payments at one level, so I don't want to pre-empt the government—how would the PSOs and other measures operate in the scenario that the senator has laid out?

**Mr Hansford:** In a preventive sense, the PSOs will allow us to work to try and proactively prevent risks through the risk management program. In a reactive sense, the action directions could be used, for instance, to direct the removal of a trusted insider. That's a physical example of someone who might be a threat to a system related issue. But, in terms of the intervention and assistance by ASD, 35AC specifies the types of acts and things that can be undertaken, which I think largely relate to IT and computer related assistance.

**Senator KENEALLY:** Directing people not to pay a ransomware or to pay it, so that then you can follow the trail—that's not part of this legislative regime?

**Mr Hansford:** The direction would have to be reasonably necessary for the purposes of responding to the incident and proportional and technically feasible, so I think you could have a scenario where those types of scenarios could be contemplated within the action directions.

**Senator KENEALLY:** What about indemnities?

**Mr Hansford:** For the direction, the immunities—not indemnities—apply. So the relevant entity and its staff—

**Senator KENEALLY:** I would appreciate some additional information about this, on notice. It doesn't feel like I have a full sense of this, or a full answer to these questions. I think some later colleagues have similar questions—we've all had similar scenarios put to us.

**Mr Pezzullo:** We'll deal with them in the supplementary advice.

**Senator KENEALLY:** Right, thank you. Chair, I'm mindful of the need to share the call. I'll flag that I have other questions and would like the call again before we adjourn.

**CHAIR:** Sure. We'll go to Senator Fawcett then we may come back to you.

**Senator FAWCETT:** I'll start off by taking you to the Victorian Information Commissioner's submission and evidence today. They highlighted that Victorian public sector organisations that would come under this framework already have obligations under things like the Victorian information security incident notification scheme. They claim they already have a working scheme which the sector understands and they're seeking an exemption or a carve-out. Could you talk to the committee about whether this was raised during your negotiations or briefings with the states? What would be the impact of the carve-out? And why, if a carve-out is not practical, is their current scheme not suitable as part of this or an analogous system?

**Mr Pezzullo:** I'll ask Mr Hansford to speak about the question of engagement with Victorian state departments or authorities, including the information commissioner there. I'm just struggling to recall the capacity and capability—and, indeed, the existence—of the Victorian signals directorate. I'm not really across the capability of the government of Victoria in the area of signals intelligence and offensive cyberoperations. But perhaps Ms Noble can assist me in that regard. While she's gathering her thoughts on her Victorian counterpart agency, I'll ask Mr Hansford to address the question of consultation.

**Mr Hansford:** The first point is that I can assure you we spoke to the states and territories, including Victoria. I think that was fortnightly Mr Grunhard? So we had lots of engagement with the states and territories in the development of the bill.

The Victorian regime really only focuses on information; it's not an all-hazards regime. So the first hurdle is that it's deficient in that respect—it's one-dimensional. The second point is that if there's an existing regulatory regime which, for instance, adheres suitably to the positive security obligation then the codesign process of the rules will be used and, indeed, can be cross-referenced and added to it. In terms of the Victorian legislation: it's

very specific but we can look at it in the codesign of the rules, add to it and put it in as part of the positive security obligations. In that way, the entire bill is meant to be intraoperative with other regulatory systems—not to be duplicative of but additive to.

**Senator FAWCETT:** Thank you. Secretary, I'm aware that your tongue was firmly in your cheek when you were talking about Victoria's ASD. But for the purposes of the committee's inquiry and evidence as we formulate our report, could you or Ms Noble talk about the impact of the information commissioner and others not having access to threat information?

**Mr Pezzullo:** They regulate a particular scheme that, quite properly, falls within the Victorian jurisdiction in relation to the handling of information. I'm not familiar with the statutes they operate under, but common sense would suggest they relate to privacy and information protection obligations, and, potentially, access to information. I'm not sure what their remit is and whether they're also the FOI commissioner in relation to Victorian state records. It's a very narrow—and I would contend, respectfully, almost inconsequential—part of this equation. To the extent to which the Victorian parliament has, for instance, set up operating arrangements through statutory schemes for those who provide power, water and gas into the state of Victoria, I suspect that the government of Victoria—and I'm fairly familiar with their views because we consult with them at a classified level, with their Premier's department and others—would be the first to say: 'We have no tools, we have no powers and we have no idea of the world beyond Victoria in terms of cyberthreat actors. We're entirely reliant, not just on the Commonwealth at large but specifically on the Australians Signals Directorate.'

So my tongue wasn't entirely in my cheek. The remit of that statutory officer is what it is. I'm sure they do very worthy work which deals with a relatively small and, for many other purposes highly consequential but for this purpose, almost inconsequential aspect because locking down your information and your driver licences et cetera is really important from a privacy point of view. But what we're focused on are the networks, the devices, the systems where that and similar data is aggregated and stored and indeed can be attacked and accessed by threat actors that are well beyond Victoria's reach. They've got a very valuable role to play. It doesn't matter whether it's state, territory, Commonwealth or other frameworks—obviously legal frameworks within those nine jurisdictions, if you include the Commonwealth—we'll use, badge and label any relevant statutory regime. We'll say: 'Right, you've acquitted your obligations to that commissioner or to that office and that, for the purpose of avoiding duplication and reducing red tape, is satisfactory for your PSO in relation to that element,' which might be, for instance, the security or the privacy of data. 'But you've done nothing otherwise that we can see in relation to protecting your network at scale from blocking threat actors by having suitable and adequate cybersecurity on your network.' We would consult with our colleagues in ASD and it wouldn't be the case that we would seek to regulate the work of Victorian agencies or departments. But their utilities—and that's why we have been consulting with the states and territories—that provide Victorians with goods and services and essential services like, particularly, banking, power, gas, water et cetera would certainly fall within the scheme because it's purely and simply a matter for federal parliamentary competence under the constitution. Ms Noble, do you want to add to that?

**Senator FAWCETT:** Thank you.

**Ms Noble:** I'll simply say that the most excellent case study and experience that I mentioned an hour or so ago was with the Victorian government. We have a fantastic collaborative relationship with our tech counterparts in the Vic government. We have formal forums through the national cybersecurity committee to work with all states and territories, including making collective decisions about a national cyberthreat alert level and about taking national activities together in order to mitigate threats like the recent Microsoft Exchange issue. That was something that we did in collaboration, so at the technical level we have a terrific relationship. The sorts of things that this legislation envisages do already occur between us and the state and territory governments, and we're very grateful for that. The final point, I suppose, is that in order to genuinely protect Australia from cyberthreats, we need a much better national picture than we currently have, which is based on the goodwill and volunteerism of state and territory governments and also some incredible private sector colleagues across Australia. But if we're really going to protect ourselves in a cyberwar, to put it in colourful terms, then at the very minimum level we need better information about what's going on and who's having a go at our country. That's a really significant part of this legislation, so to cut whole state governments from being asked to assist us with what's going on in their state would really diminish the national impact of this legislation.

**Senator FAWCETT:** To finish off on the evidence from the Victorian Information Commissioner, they raised the existing framework, such as a protective security policy framework and the Information Security Manual. They contend these are well understood by industry and their view was that legislation building on those

two frameworks would be a better use of resources than a brand-new scheme. I'm imagining your answer will go against the issue of scope, but would you be able to address their concerns in that regard?

**Mr Pezzullo:** Those frameworks are administrative frameworks that are directed by a ministerial authority. They don't directly, themselves, have a legislative basis, except insofar as they are binding on people such as me and Ms Noble through the PGPA Act and our general obligations as chief executives of departments and agencies. There has been an extension through the defence procurement program, as you would be well aware, in terms of the defence security program, that effectively imposes similar and in some cases more-onerous obligations. But, again, it's not directly in law. In that case it's part of a procurement program.

The concern we would have in terms of building on the PSPF and the ISM is that, valuable documents that they are, with all the best practice of government agencies—with all the tools that we have and the support that we have from ASD—just doing that alone, we're constantly, as Ms Noble said, in hand-to-hand combat with these actors, and we've got the best systems and the best data going around. To think that you could not regulate the private sector—which, through several decades worth of the transition of essential services from effectively public utilities and publicly owned enterprises to privately owned and operated enterprises; I make no comment about the policy direction—with the exception of the defence industry, because you're using the purchasing power of the defence investment program to require obligations through contract, and to think you could roll out a framework that was aspirational, suggestive, 'please do it', 'it would be nice if you did it' would not be commensurate with the threat that we face.

The inflection point occurred about five years ago, with WannaCry, NotPetya and some of the major attacks, which are repurposed offensive tools. The window is closing. If we were to keep watching the problem and then coming back to this parliament in a year or two to say, 'We tried the advisory route and we tried the suggestive route, the PSPF-ISM approach, and now the catastrophe has hit all sectors constantly, persistently every day,' we wouldn't be doing our job. I think we need a new scheme that in fact builds on legislation. The Security of Critical Infrastructure Act already exists, but it's very narrow in scope and very bounded to particular purposes that addressed matters that the parliament considered back in 2017 and 2018. We need this scheme, which, frankly, would pick up, for instance, whether a defence industry firm had already complied, through the contractual lever, with all of the things that Secretary Moriarty requires of them through the—you will have to help me here Ms Noble: it's the Defence Industry Security Program, I think—

**Ms Noble:** Yes.

**Mr Pezzullo:** If they've already done those things, to Mr Hansford's earlier advice, we can, for the purpose of a PSO, tag it and say, 'Right: as we map all the criticalities, that one's done, because this firm—which is in a contractual relationship with the Department of Defence to provide munitions or weapons systems to the ADF—has already done these things.' But even there, ASD might say, 'We've looked at it, we're pretty friendly with that company and they still need to do more things.' We would contend to this committee in evidence that you need a statutory scheme for transparency so that everyone knows the rules and, frankly, shareholders and directors and CEOs can say: 'The obligation's there in law. Let's now get on with it.'

**Senator FAWCETT:** Thank you. Perhaps I can move on from the Victorians. I appreciate your deep regard for the aviation industry. Having been a professional pilot before coming to this place and indeed being involved in the regulation of flight tests, I'm familiar with aviation regulation. But, to pick up on Senator Keneally's point, there are situations where even with co-development of regulatory frameworks and standards there is a place for the industry to be able to come forward with their preferred approach to meeting the intent and outcomes required by the regulation and the regulator really being able to prevent that only if they have a justifiable safety case to indicate that, for reasons known to them, it won't work.

**Mr Pezzullo:** Yes.

**Senator FAWCETT:** I'm just wanting some assurance that that's how you see this playing out, as opposed to Home Affairs and ASD imposing a solution in every circumstance upon industry players.

**Mr Pezzullo:** I can give you this absolute assurance—and I give it in evidence, and Director-General Noble can speak for herself, but I am sure she will be of similar mind—that, frankly, in the race that we are in against the adversary we can't afford to do any nugatory, unnecessary work. To take the example of the Defence Industry Security Program that I just mentioned, in its physical dimensions related to security clearances, citizenship requirements and access controls into sensitive facilities, that is a sector that is covered. We will not redo that work, because we will have a conversation with the Department of Defence as the regulator—they achieve that through contractual leverage through procurement—and we'll just double check with ASIO, ASD and others to make sure that there are no additive features. Then we're done, because we then need to move on to those sectors

where perhaps the regulatory schemes are not as deep and the co-design is not as advanced and matured. We'll focus our efforts where it's best done. Mr Hansford gave an example earlier in response to Senator Keneally, where, under the Banking Act, APRA, not waiting for this—and I applaud Mr Byres and his team for getting on with it—put down direction 234. Direction 234 under the Banking Act is a very suitable piece of direction which was developed through the APRA consultative process with the banks. And I know for a fact, because I've spoken with Mr Byres, they do sit down with the banks and the banks say: 'Actually, we've invested a lot. Here is our preferred way of dealing with the problem.' We'll come along and not come over the top and say, 'No, start again.' Our starting point in the banking sector, which is regulated by APRA, will be to start with direction 234. We'd be very keen to hear, along with our colleagues in APRA.

In each of these sector-by-sector engagements it'll be Home Affairs, ASD, plus the regulator, so we won't have to redo our homework. If the banks, in that case, say: 'Actually, we've consulted across banking across the world and we've actually got a different and preferred way of doing things which still meets the intent of 234 as well as any prospective rule the Minister for Home Affairs might make,' we consult with Ms Bradshaw. She might say, to your point, Senator: 'At this marginal area where the banks don't have the top-secret signals intelligence that we can see, we suggest this additive feature or this modification or this supplementary feature,' and Ms Bradshaw, in the consultative process, will then come back to us and say, 'But the rest of it, the 98 per cent or 99 per cent of the sector's preferred model, is acceptable to us.' We're not going to redo that homework, because frankly we don't have the time.

**Senator FAWCETT:** Moving onto paragraphs 73 and 74 in your submission, you make it clear in 73 that this is an 'all-hazards risk management' approach 'to support the nation's prosperity and security' and, in the subparagraphs, it will go to 'resilient critical infrastructure and systems of national significance'. In paragraph 74, you go on to say that '

Mature sectors will benefit from an uplift in their supply chain, as well as the networks and systems that they depend on.

You'd be aware of the work of the Joint Standing Committee on Foreign Affairs, Defence and Trade looking at supply chain resilience. You'd be aware of the executive orders from President Biden around supply chain resilience, and, in fact, the creation in the budget of an office in Prime Minister and Cabinet to deal with supply chain. I am interested in two parts. The first question is: do you see that the measures in this bill could extend to the concept of how companies that are systems of national significance, so health systems and others, actually give some assurance of resilience in the supply chain, to have a framework of how to assess it and how to make sure that their measures are suitable and effective? The second question is: given your role in interfacing with state governments and the private sector through the Critical Infrastructure Centre in Home Affairs, do you see a role for Home Affairs and the Critical Infrastructure Centre in that ongoing engagement, management and regulation of supply chain resilience?

**Mr Pezzullo:** The short answer is yes. I'm still giving this some thought, but, just to foreshadow the likely changes, we'll put in place to give administrative effect to this scheme should the parliament provide these powers to the department and the minister. We will in fact go further than the machinery of government changes that were instituted in 2017 by former Prime Minister Turnbull, where we brought together critical infrastructure, cybersecurity and, critically, emergency management. I don't want that element of supply chain and national resilience excluded from my answer, so I mention them, not in terms of the immediate first responder to fires, floods, and cyclones—that EMA role is well understood—but noting that, off the back of the pandemic, we have evolved and will soon institutionalise it through a new crisis management framework for government to consider the national coordination mechanism for, if you like, in-flight supply chain issues, in-flight supply chain resilience issues. We will be working with that office in PM&C that you just indicated.

Of the three big tools we have, the critical infrastructure centre, which goes to infrastructure security, was born out of a physical infrastructure security legacy, but I'm thinking about how I reconfigure administratively a cybersecurity and infrastructure security function. The EMA component of supply chain resilience is a more immediate crisis response function—power is out because of a storm; supply chains have been broken because of some natural calamity or, potentially, a human calamity. Of course, the cybersecurity rules and obligations that we will generate through this act should be passed by the parliament won't solve the entire problem of supply chain resilience, as you well know. I wouldn't want to even begin to give you any advice on supply chain resilience. You have made it a key feature of your time as a legislator and as a committee member.

But whether it is fuel security, whether it is manufacturing, whether it is the defence industry, you well know that there is a whole series of levers, some of which relate to things like industry policy, R&D, government grants and procurement strategies, which are outside the remit of the three main functions of my department. But to the extent that this legislation would give us another weapon, or another tool, shall I say, to bolster not just an

immediate cyber incident response—we have spent a lot of time in this hearing thus far on that—but also in relation to, in the physical world, the ability to ensure and underpin fuel supply continuity, food and grocery continuity. You saw the work of the NCM, for instance, around supermarket distribution issues through the pandemic.

Yes, this legislation, the PSOs, the positive security obligations, typically—mainly it is through the PSOs—give us another tool in that strategy. That said, I want to emphasise that a number of other colleagues have a co-equal and, in fact, some cases, leading role in energy security under the energy minister, the industry policy aspects of supply chain resilience under the industry minister, and given at the office is in PM&C and has been announced to be in PM&C for the foreseeable future, the Prime Minister himself will take the lead on supply chain resilience. So we all contribute to that broader complex set of problems which do require you assembling a series of tools. And, yes, this tool, quite outside of the IT, OT and cyber capabilities that it will afford us, will also help address some of those supply chain issues.

**Senator FAWCETT:** So in terms of coordinating all those stakeholders you have mentioned, let's look at health as an example. This bit of legislation expands the concept of infrastructure into systems of national significance and includes health within that. We had evidence from the pharmaceutical industry, for example, around the significant risks to the Australian population of supply chain disruption due to pandemic cyber emergency or other things to pharmaceuticals and the APIs that lead into their manufacture. Are you going to have mechanisms, like SCONS, for example, that will be the coordinating body across those various arms of government? Who is going to take the lead to make sure the security supply chain resilience pieces and manufacturing are actually in this case tied up in a health outcome?

**Mr Pezzullo:** I can give you a direct answer without speaking for the Prime Minister or the Department of the Prime Minister and Cabinet because I can speak to lived experience. It is certainly this Prime Minister's approach, and he has made it very clear, to use the National Security Committee of Cabinet, which is supported by the Secretaries Committee on National Security. I have the honour and privilege of serving on both committees. He sees the concept of national security and the utility of both the cabinet-level body, the NSC, and the secretaries' level body, the SCONS committee you made mention of, as having a very expansive role in relation to national resilience, supply chain and sovereignty issues, as well as the more classical national security issues that arise in relation to espionage, military threats and the like. The Prime Minister, who has spoken about this publicly, so I'm not breaching any confidences here, has tended to use the NSC before matters get to national cabinet. I won't include national cabinet in my answer. He certainly used for pandemic response in Australia an augmented NSC, which involves the health minister and at times the industry minister and other ministers coming on. So the core is always the NSC membership. We have the benefit, both as cabinet ministers and as departmental secretaries and a number of statutory officers, of typically reading pretty much every day the same threat information. We read the same intelligence, diplomatic reporting. We have alerts that come up either from our colleagues in emergency management in terms of natural hazards, from the Australian Cyber Security Centre and ASD on cyber. Obviously Defence keeps an eye on any military developments of concern and so on and so forth. If you will, that is the engine room for situational awareness as well as supporting government decision-making. Secretary Gaetjens, as the chair of SCONS sitting under NSC, very much uses SCONS, as a number of his predecessors have done—I shouldn't suggest otherwise—in a true, all hazard sense whether it is a pandemicor otherwise.

Without going through the full list and certainly not in terms of anything I shouldn't speak about publicly, we have looked at certain naturally occurring discontinuities that would be of catastrophic consequence. Geomagnetic storms that, for instance, would render satellites inoperable, what would that mean in terms of dealing with the catastrophic impact? So national security in that sense is not related to an attacking military force or a foreign intelligence service; it is related to a natural event that is well beyond the capacity of any state, territory or municipal authority to deal with.

I will finish on this: the flexibility in that committee, because it is chaired by the Prime Minister at one level and the secretary of PM&C at another level, means they can co-opt any experts they wish to co-opt subject only ever to security clearances and the need to know. So that gives us both a stable core and a very flexible mechanism by adding in other portfolios and agencies as required. My personal view, and I am only expressing this personally, is we can only improve on that machinery; you can always improve. I wouldn't set it aside and design anything new; I would build on that NSC SCONS machine.

**Senator FAWCETT:** Obviously the drafting of SOCI was some time ago, not a long time ago. A lot has changed through the whole experience of COVID. As you've indicated, new mechanisms and frameworks have been stood up to deal with that. Are there any aspects of this piece of legislation where, in an ideal world and knowing what you know today, you would like to see amendments or improvements that would help facilitate

Home Affairs and Critical Infrastructure Centre's work as one part of this national approach to ensuring supply chains?

**Mr Pezzullo:** It is a very tempting invitation. As you rightly say, this is the second version of this legislation. There was a precursor bill in 2017, an act of parliament in 2018. It was more narrowly focused—you're absolutely right. Even in the last three years, both in terms of natural hazard and extreme weather risk but also in relation to the cyber risk, I described it as a global pandemic that is emerging in relation to cyber. I use that term advisedly given what I know, largely based on the excellent advice, the wonderful advice, we get from the director-general and her staff. I shan't take full advantage of your invitation as to what SOCI III might look like as we get into this cycle of collaboration, codesign, hopefully proactive and preventative measures. To go back to one of the points I made to Senator Paterson, if we're negotiating through lawyers and through the general counsel when the catastrophic impact occurs, to some extent we wouldn't be using the full scope and majesty of this legislation to get into the continual improvement, collaboration and collegiate co-design of solutions to problems—the principles that Ms Bradshaw spoke about—because, frankly, we don't want to be turning up when everything is destroyed or near destroyed.

The only thing that I would suggest to this committee is worthy of at least marking intellectually and in a policy sense for further consideration down the track is: notwithstanding that some submitters described the government assistance measures as potentially involving overreach—we would contend that they're probably on the lighter side of proportionality—if we just keep getting attacked, and I dealt with the question of state enabled, state sponsored, state tolerated cyberactors operating effectively out of pirate havens, there will be some issues around offensive strategies and authorities that I prefer to not speak about directly; in any event, they wouldn't be anchored in this legislation or any subsequent version of it. But I do potentially contemplate, and colleagues in the United States have started to talk about this—it was actually a feature of President Biden's critical-infrastructure legislative package, most of which has been focused on roads, bridges, and rebuilding America's infrastructure—there are some digital infrastructure measures that I would draw to the committee's attention, where I think, in the future, we might need to go further. I venture this purely because you've invited me to, not so much as an opinion, but as a view that I might put to the committee for future consideration.

If the government assistance measures don't work sufficiently robustly, we might need to start thinking about how, as new networks, cloud and other capabilities are deployed in utilities, telcos, banks, we actually design, from the ground up, and partner with them, using the mechanism of the GAM, the government assistance measure, to help them more securely co-design their networks as they build and evolve their network. A bank might, for instance, engage in a significant transformation of its online presence. They might come, in any event, to Ms Noble and Ms Bradshaw, because it's good practice, or they might be obligated to submit future concepts under a PSO and say, 'Rather than having this antagonistic our lawyers will show your lawyers this, why don't you help us think about what a more secure network looks like?' It might become the case—and I think the market will start to form in this way—that new configurations of essentially commercial intranets, heavily protected secured intranets, start to emerge, which become operating platforms for different sectors, particularly those sectors that have key interdependencies for the whole of society, like the banking system, for instance.

I don't want to go ahead too far ahead of where that discussion might go, but that would increasingly increase our sovereignty and our supply chain resilience as well as the resilience of our cyber-ecosystem. I'm not suggesting for a moment, sitting before you speaking about this bill, that we need another bill. What I would say to this committee, in the interests of full transparency, is that, over the next few years, as we see this cycle of obligations, reports, co-designing of rules et cetera, and as we still see the attackers getting through, it might be that you start to get to a point where more secure platforms have to be thought about.

As I read the statute—and it's been in the back of my mind as we've worked through the development both of the legislation and all the explanatory materials—we've got sufficient scope within the government assistance measure to start to eke out that terrain. You asked me about future requirements. It might be that, in years to come, if not sooner, we're before this committee with yet more protections that we need to build in, because through this struggle—I think Ms Noble talked about daily hand-to-hand combat—we are constantly learning what the attacker can do, and they're learning about our responses. They're going into new havens that we haven't yet discovered. So it's going to be a constant dialectical to-and-fro.

I certainly would not suggest for a moment that there are deficiencies in this bill as we've put it up. We would never have put the government and the parliament in that position, but I can intellectually see a case, because you've asked me the question, for some additive measures to be built onto this regime, which I think will, over time, like other foundational legislation such as the Foreign Acquisitions and Takeovers Act—here we are, four

decades into that journey, still thinking about how we refine the operations of the FIRB and the obligations and measures under that legislation, which is, if not over 40 years old, pretty much almost 40 years old.

**Senator FAWCETT:** Thank you.

**CHAIR:** We'll go quickly to Dr Aly and then to Senator Keneally for her further bracket of questions.

**Dr ALY:** I just have one question for Mr Pezzullo and then one for Ms Noble. I will start with you, Mr Pezzullo. One of the other submissions made reference to the definition of 'cybersecurity incident' in the bill and specifically pointed out that the proposed definition in the bill only looks at unauthorised access but doesn't really cover insider threat or human error. I noticed that you referenced Homer Simpson earlier. That would be the kind of human error we're looking at here where an incident could be accidental or it could be deliberate but deliberate by an authorised person. I would wonder if you could comment on the definition of 'cybersecurity incident' here and whether you feel it adequately covers insider threat and human error.

**Mr Pezzullo:** Certainly it would be our contention that an insider threat situation, whether it's a foreign agent or an external party that has got human access into your organisation and then is infecting through putting devices into drives and the like—so that's an insider, but that is a hostile or malicious action which is intrinsically unauthorised. By definition it's unauthorised. It could be a disaffected employee. We would argue that's unauthorised. There are very strict rules and procedures that most companies and certainly government agencies have about their administrators who have got administrator rights and so on and so forth. But there could be someone who abuses those rights. We would think that's covered. As to human error—

**Dr ALY:** Sorry, Mr Pezzullo. You said they would be considered unauthorised?

**Mr Pezzullo:** If they're operating beyond their legal duty. Say you've got an administrator who's got quite extensive reach over a system. They're paid to be an administrator to keep the health of the system up so that the business can keep running and the essential services—for instance, the transition of electricity—can keep running. If that insider—and we'll get to error in a moment—says they are maliciously, deliberately motivated illogically, motivated by money or motivated because they've been activated by a foreign power to engage in sabotage, we would say that's an unauthorised use of the employment privileges that that officer has. Whether it's an administrator, a superadministrator or, indeed, any employee or member of our staff without even those administrator rights who infects a device or infects the network, that would be malicious and by definition, therefore, unauthorised.

But I wonder about error, Mr Hansford. You don't need to use the Homer Simpson example if you don't wish to!

**Mr Hansford:** I think that's the whole premise behind the risk management plan, which puts the obligation on asset holders and entities to identify where there's a material risk that the occurrence of the hazard could then have an impact on the availability of the asset. The next step is, so far as possible, to mitigate or eliminate that risk. One of the risks may well be a trusted insider or someone acting maliciously. Then it is to make sure that that mitigation is appropriate. So it's a principles based risk management plan bespoke to the asset and covering all risks that can then be mitigated, which then flows into how if you don't mitigate then one particular area that might occur is a cybersecurity incident. Then you get into the definition of the incident. So there are two separate concepts. One is about risk management, including all hazards, which includes, to Senator Fawcett's point, supply chain security, personnel security as well as protective security.

**Mr Pezzullo:** So continuity of the service would be covered.

**Mr Hansford:** Indeed. It's all about the protection of the asset and the functioning of the asset.

**Dr ALY:** With specific reference to the definition of 'cybersecurity incident' in the bill, I know, Mr Pezzullo, you talked about unauthorised abuse, but what if the access is authorised? Is that not different from unauthorised access? Someone may have the authorised access. Yes, they may use them in different and malicious ways, but they still have the authorised access.

**Mr Pezzullo:** Typically, you see this with phishing campaigns and clicking on malicious links. The payload still has to come out of the network. This goes to error to some extent. We have it in our own organisations and we have to very quickly quarantine and contain the spill out of the malware. I might ask Ms Noble to assist me with any further evidence on this point. But the access might well be authorised. Either the officer or the employee might be duped or through social engineering might feel that the information that's being presented to them—for instance, in an email—is legitimate. They click on a table or a spreadsheet and they activate the code. The attack is the malware.

So the access in that case would of course be legitimate. You're doing your work. You're paying an invoice or you're responding to an email. We have seen incidents, I think, where staff have received an email from what they thought was their boss or, indeed, the chief executive of the company. It all seemed to prove up. There was social engineering to put some features into the message to give a suggestion to the employee: 'Yes, it is from Dr Aly, our chief executive. She sent some information. I'll forward it on' or 'I'll click a link.' The attack starts with that grooming or social engineering that convinces the person to click. They're not part of the criminal conspiracy. Then the malware starts to deploy. That's the attack.

**Mr Hansford:** 12M covers the definition. Is there a particular suggestion about amendment?

**Dr ALY:** I'm actually referring to a submission that was made by someone else, but I will have a look at that and perhaps put something on notice. Thank you.

**Mr Pezzullo:** Very quickly: the point is well understood and made. A cybersecurity incident is one or more acts, events or circumstances involving any of the following: unauthorised access to a computer program, for instance. In that case, the employee has got the authorised access but they're the one who are duped, or they could be a saboteur who is activated. So the access is still authorised, because as far as the company is concerned it's a valid employee with computer access rights. They've got an issued device; they've got a laptop or whatever they've got and a log-on. As far as the company is concerned, that is legitimate. All it does is then open the window for the burglar to get in.

**Dr ALY:** For the unauthorised.

**Mr Pezzullo:** That's right.

**Dr ALY:** Thank you. M Noble, I noticed that you used the term 'cyberwar' in one of your responses. I want a little bit more information from you on that. Given that cyberwar is a fairly contentious term in itself and that it really refers to acts that are quite forceful and that are violent, instrumental and attributable under the definition of 'war', I wonder if you could speak a little more about this threat of cyberwar from either state or non-state actors. Is this something that is a real and impending threat?

**Ms Noble:** In the context in which I use that terminology—and I said before it was fairly colourful to use it—I was sort of referring to that notion in the broad. I think it's an experience that Australia is actually having at the moment. There is a complex array of actors operating to diminish, harm, steal from or spy on all parts of the Australian economy, from Commonwealth government, state and territory governments, major corporations to small businesses and individuals, who are tricked into, as Secretary Pezzullo said, giving away their life savings in a car scam. I was referring to it in the broad sense and saying that there are just thousands of these activities aimed at Australia at the moment. It's chaotic, it's hard to get a clear picture of it and it's hard to understand who are the big players, who are the little players, how to go after them and who to confront. I was talking about it in a general context of the chaos, the fog and the feeling of the complexity that war can present.

**Dr ALY:** That really does clarify it, so you're referring to a landscape of war-like activities?

**Ms Noble:** Yes.

**Dr ALY:** Thanks so much for clarifying.

**Senator KENEALLY:** The bill deals with critical infrastructure and essential services. Does the government have a set of criteria or a protocol about when to notify the public that critical infrastructure or an essential service is under attack?

**Mr Pezzullo:** As with any other national security related matter, in the end it's a question for judgement and ultimately escalation to the National Security Committee of cabinet or, in a crisis, perhaps a smaller group of ministers. There certainly are written procedures that the head of ASD, I and others follow in terms of crisis or cyber-response. There are standing groups that support the secretaries committee that I mentioned earlier. There are standing groups that relate to the threat environment. This is before you get to very tightly controlled procedures around attribution that relate to Australia's diplomatic interests.

**Senator KENEALLY:** I'm not asking about attribution.

**Mr Pezzullo:** Understood. We have a cyber-response board process. Typically, for something serious it would be headed by a band 3, so one of our deputies. Depending on the scale of severity, it would quickly get into the Secretaries Committee on National Security and the National Security Committee. We, on the civilian side, so outside of wartime, co-lead with our colleagues in ASD. Obviously, in the context of war, the CDF takes over.

**Senator KENEALLY:** I have a range of questions here. Does the government have a protocol for determining how and who should make the public notification, if there is a decision to make a public notification?

**Mr Pezzullo:** Yes, it's laid out in correspondence. I'd have to refresh my memory as to timing. Certainly, it's this Prime Minister's preference that it be done conjointly. Leaving aside a diplomatic aspect, an attribution to a foreign state where the foreign minister gets involved, typically it's left to the defence minister and the Minister for Home Affairs.

**Senator KENEALLY:** You said that's laid out in—

**Mr Pezzullo:** It's either in correspondence or in a minuted decision of government that relates to our cyber-response arrangements. I'll have to check on notice the exact flow of correspondence and I'll come back to you on notice.

**Senator KENEALLY:** Yes.

**Mr Pezzullo:** And then the Prime Minister has always got the discretion, as the Prime Minister, to step in himself. You saw Mr Morrison do that last year, with an announcement about the sophisticated state actor on Australian systems.

**Senator KENEALLY:** Very good, Mr Pezzullo, you have anticipated where I'm going. Mr Morrison said he made that announcement on 19 June 2020 'to raise awareness' and 'encourage organisations, particularly those in health, critical infrastructure and essential services, to take expert advice and implement technical defences.'

**Mr Pezzullo:** Yes.

**Senator KENEALLY:** Essentially, he was doing a notification to operators of critical infrastructure and essential services to ensure they had appropriate cyberdefences in place.

**Mr Pezzullo:** We asked him to. Ms Noble and I and a number of other key colleagues in the national security community said, 'Prime Minister, this is so persistent now and so critical.' It's obviously the Prime Minister's discretion as to where he applies his authority and his weight, but we encouraged him. I have to say he was very positively inclined to do it, and we obviously briefed him. Ms Noble and her staff briefed him on the detail. As you saw with Operation Ironside the other day, in a completely different context, with something that is impactful on the whole of society—and this is a matter always for judgement by the Prime Minister of the day—when you associate a Prime Minister with an announcement like that it just gives it additional impetus, focus and consciousness-raising over and above what one or two ministers would do. I know that there's a very interested readership of Ms Bradshaw's advisories. It really does amplify those technical advisories to the power of the Prime Minister.

**Senator KENEALLY:** Mr Morrison, though, didn't just make a public notification on 19 June; he provided a commentary about his track record as Treasurer and then Prime Minister in terms of investing in cybersecurity. He restated previously announced government positions, he flagged new announcements that were coming from his government and he spoke in what fairly could be described as political terms. Are you aware that in the United States there are defined policies and procedures to ensure that notifications like that are done not by an elected official but by a national security agency—namely, the FBI and Homeland Security?

**Mr Pezzullo:** That component of Homeland Security is very well known to us—the Cybersecurity and Infrastructure Security Agency. They put out technical advisories pretty much daily. Ms Bradshaw plays that role here in Australia; she is the technical advisor to Australia. But you could make the same argument about a prime minister or a minister standing up on any announcement; they could send an official out on anything. It's really a question of when they decide to apply the weight of their office to the matter.

**Senator KENEALLY:** There is a difference, though, isn't there. With Operation Ironside, something had come to a conclusion of sorts and an announcement was being made about an outcome. Here we had a circumstance where national security agencies had determined certain information needed to be provided to the public in the context of what was described as an ongoing attack. Sure, you could make the claim that any announcement by a government minister is necessarily political. But in the context of providing information about a national security matter that is ongoing, and issuing notifications and seeking certain actions from the public—and I'm thinking about the history of ASIO and the politicisation of national security agencies—there might well be a risk. It looks like national security information is being politicised by whichever party is in government—if there is not a clear separation between necessary national security information being provided for community safety and political messaging

**Mr Pezzullo:** I'm not sure if you're asking me to comment on political strategies, communication and messaging. I'm not really an expert in that field.

**Senator KENEALLY:** No, but as Secretary of the Department of Home Affairs you are an expert on our national security agencies and the way we ensure they are not overly politicised. Particularly given the history of politicisation in some of our national security agencies, I think we have to be on guard about this in this country.

**Mr Pezzullo:** As matter of principle, certainly those of us who work in this sector—and I have done so for three decades—always prefer the least amount of politicisation and the maximum amount of bipartisanship. In saying that, I don't really accept the premise and it is not really for me to accept or deny it. You say the Prime Minister was being especially, particularly or in a supplementary fashion political, as you define it, on 19 June. That is a matter that I would ask you to direct to a minister. There is no minister at the table. I'm not going to comment on the Prime Minister's choices.

**Senator KENEALLY:** I don't expect you to comment on them.

**Mr Pezzullo:** But as to the technical question about who should do the advice—Director-General Noble and I discussed it extensively—it was our idea, along with a couple of other colleagues, to say that this is now so persistent. Ms Bradshaw had put out a number of advisories. We were particularly concerned about the sophisticated state actor, the details of which I won't go into—and to this day we have never identified that actor.

**Senator KENEALLY:** I'm not asking you to.

**Mr Pezzullo:** Indeed. But the geopolitical, commercial, consumer and public safety consequences were so severe that having the weight of the nation's leader—in effect the person who occupies the office of Prime Minister—was important. What his motivations are and what your interpretations of his motivations are is not really a matter for me, and I know you're not asking me to comment on that. But, I thought, as someone who was one of the people who asked him to do it, it was entirely reasonable. I would have done it irrespective of party; the colour of party is of no interest to me at all. But it's no different from—

**Senator KENEALLY:** Still—

**Mr Pezzullo:** Sorry, just very briefly if I could conclude: I don't see it as being any different from the Prime Minister—not Mr Morrison, but any Prime Minister—or the Health minister standing up to give public information on a pandemic. There might be a separate argument about, in a pandemic sense, certain public information that relates to health safety, and then you can add a political debate about vaccine rollouts and all the rest of it, but that's separate.

**Senator KENEALLY:** And, indeed, to take your analogy—

**CHAIR:** Senator Keneally, can I jump in very quickly, on the chair's indulgence. I am seeking a brief answer, because we are over time and I want to go back to the Senator Keneally, but perhaps, Ms Noble or Ms Bradshaw, you could briefly illustrate what the post-effect of that announcement was, what was the consequence and what were the behavioural changes you observed?

**Senator KENEALLY:** Chair, I appreciate that. I'm very keen to quickly finish. I'm not trying to get to whether or not the announcement should have been made; I'm actually trying to tease out a difference in approach between the United States and Australia.

**CHAIR:** Let's come straight back to that after a brief answer on that from ASD.

**Ms Noble:** I might very briefly try to cover both. We did put out quite a few advisories—I don't have the specific detail—prior to the Prime Minister making the announcement. Quite frankly, our concern and our advice to the government of the day, as Secretary Pezzullo said, was that not enough people were paying attention to those advisories and acting on them. With the Prime Minister lending his profile, his prerogative as the leader of the country, amplifying or drawing attention to those advisories, we subsequently saw a dramatic step change in the implementation of the technical advice that we put out, including a huge uptick in the number of companies and entities who were running the checks on their networks that our technical advice gave them and then telling us more about what they were seeing, which helped us enormously to understand the extent to which this adversary had gotten into Australia. So that was, very quickly, the impact before, at the time of the announcement and afterwards from an operational agency's perspective.

**Mr Pezzullo:** Can I address the US comparison that Senator Keneally has raised. Senator Keneally, you are right in saying that, and we'll come back to you on notice in relation to our formal protocols about the triaging and the authorisation of the advisories, which are typically anchored in the Australian Cyber Security Centre, and, then, if there are diplomatic or other matters, DFAT comes into play. But, as to the US comparison—respectfully, the CISA, the critical infrastructure and security agency, and Homeland Security—you're absolutely right. They've got a website. They've got technical advisories. The head of that agency is a direct report to the secretary of Homeland Security. It's an agency well-known to us. But I'll give you an instance in April with the Russian

sanctioned or endorsed SolarWinds attack, which was called out by the United States. I'll have to check the exact dates and references, but I've seen the President speak about it. The President, in a press conference, has spoken about it; National Security Advisor Jake Sullivan, who's, in effect, a member of the President's political staff—he's a member of the President's NSC—has spoken about it; and the Deputy National Security Advisor Neuberger has spoken about it, not to do a substitute or an alternative advisory but to amplify, with the full office of the President of the United States.

**Senator KENEALLY:** I'm not arguing that, Mr Pezzullo. I'm not suggesting that no politician ever can talk about these things. I'm talking about where the distinction should lie in a representative democracy between the provision of important national security information, particularly when it comes in the context of a warning or a request for action, and where the appropriate political commentary about it sits.

**Mr Pezzullo:** I fully understand the point.

**Senator KENEALLY:** To quote the United States Senate Committee on Armed Services' testimony from Cyber Division assistant director of the FBI Scott Smith:

FBI and the Department of Homeland Security (DHS) have well defined policies and procedures which guide how victims are identified and how notification should be made—

and it is done by the FBI and Homeland Security. Other things that come afterwards are political commentary or political leadership, but it is not the role of the political actor to make the notification. hat's what I'm trying to tease out. It might be right or wrong to do it that way, but that's what I'm trying to understand from the policies and procedures that are already in place in Australia.

**Mr Pezzullo:** I understand the point, Senator. All I would echo is that our system very much mirrors the American system. Ms Bradshaw had already made the technical advisories. They were read by the very technical cybersecurity community some days, if not, weeks before, I think. You're right: in Australia, it would be a matter for the Federal Police Commissioner to stand up and announce it, as he did the other day—and, yes, the Prime Minister and the home affairs minister were standing next to him. It would be up to our FBI equivalent, the AFP, to announce major arrests and the bringing of charges—

**Senator KENEALLY:** And that's a different thing.

**Mr Pezzullo:** Yes. If I could contend respectfully, Senator, under law it's the Director-General of Security and no-one else who provides the security assessment and the threat advisory to the Australian population in terms of the probability of a terrorist attack.

**Senator KENEALLY:** That's right.

**Mr Pezzullo:** That's actually set out in statute. But that doesn't prevent the Minister for Home Affairs speaking—

**Senator KENEALLY:** That's precisely the point that I'm trying to understand—why that occurs in ASIO. Why doesn't the home affairs minister give the director-general's annual threat assessment, then?

**Mr Pezzullo:** It's codified, in the case of the ASIO Act, that the Director-General of Security is personally accountable and cannot be influenced in the performance of that function, as it is the case for the Director of Public Prosecutions with the bringing of charges, and the AFP Commissioner. We've all got statutory roles. It's then a matter for judgement—and I'm not going to buy into the characterisation of the Prime Minister's action as political, and I know you're not asking me to. You've been the premier of a state, and you would have applied your own judgement about when you stood up and amplified, explained, teased out, added to announcements made by statutory officers. I think it's just part and parcel of how political discourse occurs.

**Senator KENEALLY:** That is what I'm trying to get to: should this be an announcement by a statutory officer—a public notification of a cyberattack—or should it be made by a political actor? Let me put it to you in these terms, Mr Pezzullo. Let's say during an election campaign a cyberattack occurs on a piece of critical infrastructure or an essential service and public notification is warranted. Would the caretaker conventions make any difference to how the public would be notified of a cyberattack in that context?

**Mr Pezzullo:** The caretaker conventions are very clear as to not announcing or deciding policy that is binding on a potentially different incoming government, so, insofar as it didn't offend that principle, the advice that we would provide during an election would be the same as outside of an election. In the case of the state actor last year, the Australian community was notified by Ms Abi Bradshaw, not the Prime Minister, because several days before—or was it weeks before? I can't quite recall.

**Ms Bradshaw:** In the months ahead.

**Mr Pezzullo:** In the months ahead, the ACSC, which is a component of the ASD, put out a technical advisory. How many people read it or whether it was read beyond a technical readership is a different point. But, to your point, that advisory was made by a deputy in a statutorily independent agency, namely a deputy director-general of the ASD. To have the Prime Minister then amplify it, which gives broader reach and more awareness—Ms Noble has given evidence about the take-up of her advisory services and having more subscribers to their website—is a good thing.

**Senator KENEALLY:** Mr Morrison didn't actually reference those technical notices in his remarks—

**Mr Pezzullo:** I would have to look at the transcript.

**Senator KENEALLY:** I've got it. Go ahead and have a look. Are you saying the caretaker conventions in your judgement would make no difference if a cyberattack was occurring during an election campaign? You would you give the exact same advice to the government of the day that the Prime Minister should get up and amplify it?

**Mr Pezzullo:** The caretaker conventions are very particular about officials being obligated not to provide advice or any services to a minister that relate to decisions or policies that would be binding on the opposition, as the alternative government, save in a circumstance—and I've seen this happen during a caretaker period—where, for reasons of urgency, the minister is advised to consult with his or her shadow. In 2001 there was consultation between the then Howard government and the then Beazley opposition on some urgent matters under the Defence Act. The caretaker convention does not preclude government performing its normal functions. What it obligates ministers and officials who support them to do is ensure that extra care is taken in relation to consultation with the opposition as the alternative government.

**Senator KENEALLY:** I might invite you to have a review of the caretaker conventions and take on notice if, in your view, the caretaker conventions would require the department to provide any additional advice or consultation with the opposition if you formed a view that public notification of a cyberattack was warranted.

**Mr Pezzullo:** Very happy to do that, noting of course that my colleague the secretary of PM&C is responsible for those conventions. He's the steward of those conventions. We'll consult with him. Senator, just to be clear, I do recall the Prime Minister referring to advisories on 19 June. The statement's in front of me. I will read it. It's just a matter of fact. About halfway down the first page:

The ACSC has already published a range of technical advisory notices in recent times, to alert potential targets and has been briefing States and Territories on risks and mitigations.

Then he goes on to say—

**Senator KENEALLY:** In a general sense that is true; they do that all the time.

**Mr Pezzullo:** Indeed, but it's clear on the face of the statement, headed 'Statement on malicious cyber activity against Australian networks'. That sentence has to be read in the context of that actor.

**Senator KENEALLY:** You and I might have a difference of interpretation here as to how his various sentences should be interpreted. Thank you for taking on notice that aspect of the caretaker conventions. Having read them on the Prime Minister and cabinet's website, it does seem to suggest the departments need to interpret them within the context of their own agencies. I would appreciate it if you could take that on notice for me.

**Mr Pezzullo:** I will do so, noting that I will need to consult with the Department of the Prime Minister and Cabinet.

**Senator KENEALLY:** I think that's quite appropriate, and I would welcome additional input from them.

**CHAIR:** Thank you, committee members, for agreeing to extend, and particularly the witnesses for facilitating that. As we've reached the end of the hearing today, I want to say something about the process for the inquiry going forward, because there has been a lot of interest in it from submitters.

The committee has agreed to schedule at least two further hearings, which will be primarily focused on receiving industry feedback. We'll try to do so in a way that is representative of the sector's most affected and the businesses that have the most substantive submissions to make, but of course we won't be able to hear from every submitter. The secretariat will be contacting submitters to invite them to appear at those upcoming hearings. It may then be necessary for the committee to hold one further hearing with Home Affairs and agencies to respond, potentially, to some of the evidence that we get in those hearings. If that's the case, the committee will schedule it and be in contact.

In the meantime, Mr Pezzullo, we welcome your agreement to address those technical and drafting issues. The secretariat will liaise directly with the department to identify those priority areas on behalf of the committee. That will assist us to focus on the substantive issues and come to this as swiftly as we can while carefully considering

the substantive issues that we have to. With that, I ask that any questions taken on notice be returned by Friday 25 June. I note that the transcript, as per usual, will be provided to you for any suggested transcription error corrections. Thank you very much for your participation today.

**Committee adjourned at 15:53**