Webinar Host - Ian Gibson (DSPANZ): Okay. I think we should make a start.

I'd like to welcome everyone today and I'd like to acknowledge the Traditional Owners of the Country throughout Australia and recognise their continuing connection to land, waters and culture. We pay our respects to their Elders past, present and emerging.

And we'd also like to thank our Webinar Week sponsor SuperChoice for supporting this event.

So it gives me the great pleasure to introduce Patrick Fair who is the Principal of Patrick Fair Associates as well as an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University. He's also the Chairman of the Communications Security Reference Panel at the Communications Alliance, a member of the IoT Alliance of Australia Security Workstream and General Advisor to and an author and General Advisor in relation to LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

Welcome Patrick and thank you for making yourself available today.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Thanks Ian and thanks everybody for joining the seminar. So what I'm going to do is describe to you the proposed reforms to the Critical Infrastructure regulatory framework.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): And I propose to do that by outlining the existing rules that regulate Critical Infrastructure. And then talk about the proposed amendments. And then I'm going to talk about some of the consultations that are underway including looking at the rule making consultation that tells us about what the regulatory framework will look like. This is an important reform because it's going to expand the regulatory framework much further than it currently reaches and it matters not just for people who are actually going to be Critical Infrastructure but also for suppliers to Critical Infrastructure because you need to know what your customer, how they're going to respond to the tenders and proposals you put to them.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So first, let's have a look at what are the existing rules regulating Critical Infrastructure.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): At the moment, and this comes about through the Security of Critical Infrastructure Act which was passed in 2018, that Act regulates

certain listed ports and broadly regulates major water, gas and transmission assets. Roughly sitting in a framework where if they serve more than 100,000 people a day, then they're regulated. For electricity, because the generators share power across the grid, then a certain amount of power has to be generated for them to be Critical Infrastructure.

And the framework allows the Minister to secretly declare other assets as Critical Infrastructure. Don't know if he's done that or not but the proposed frameworks suggests that he might not have because the Government is formally reaching out now across the economy to expand the obligations that apply to this sector.

So, if you happen to be an operator of one of these assets, what do you have to do? On the existing framework, you have to give the secretary for the Department of Home Affairs operational information in relation to your asset and interest and control information in relation to your asset. And if there's a change in that information, you need to update it within 30 days. So, interestingly, just this one upfront report.

Operational information talks about who your CEO is including their nationality and key things about how the asset is operated in case there's a weakness like you've got a critical control system that's offshore or outsourced.

Interesting control information, makes you report who owns your asset plus who owns 10% of anybody who owns 10% of anybody who owns 10% of your asset. So it's quite a serious reporting obligation and that sort of thing that can just change from time to time and will require a new filing with Home Affairs to update. Likewise, changes to outsourced arrangements require updating.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): This framework is supported by aggressive powers for the Department to get information or documents and undertake an assessment of the risks associated with your asset. And, at the end of the day, if the filing you make updating who owns you or updating the way that your asset is operated is unsatisfactory to Home Affairs because they think it offers a threat to security, then the Minister can, after some steps, direct you to do any act or thing i.e. perhaps make you undo it or make you find a new operator. So very serious powers there backing up this ownership and control filing information.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): There's also a secrecy obligation which is a little bit difficult to untangle but essentially anything, any information or document about this process and the fact that you've been declared a Critical Infrastructure asset can't be

shared by you but can be quite widely shared within government. There are exceptions for it to go to the tax office, to foreign affairs, to ministers, advisors. It's an interesting dimension to the control.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's being proposed in the reform. So the reform was some legislation consultation put out by Home Affairs last year. They had a consultation process and then they sent it to Parliament where it was moved and sent off to the Parliamentary Joint Committee on Intelligence and Security.

Now interestingly, 30th September - very recently, that committee reported on the legislation. And I should tell you that the committee reported that the legislation ought to be split in two and some of the powers for the Minister to intervene and take control of Critical Infrastructure assets in a crisis plus the reporting obligations should be passed but the more aggressive regulatory stuff should not.

Now I see we've got a poll coming up.

Webinar Host - Ian Gibson (DSPANZ): Sorry Patrick. I think the poll's just popped up so we might have to cut to that.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Sure. If everybody wants to answer the poll. It's quite interesting to see what people think.

Webinar Host - Ian Gibson (DSPANZ): For those who can't see, the questions are you paying attention or monitoring this issue which is of course regarding Critical Infrastructure. And if yes, do you understand what it applies to and what your obligations are?

Webinar Host - Ian Gibson (DSPANZ): It's interesting just noticing the results of the polls there and we'll just give people a couple more seconds. So the response, what is it 75% yes they are monitoring the situation but 50% said they don't understand what it applies to and what their obligations are.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Right.

Webinar Host - Ian Gibson (DSPANZ): So it's a significant number.

Guest Speaker - Patrick Fair (Patrick Fair Associates): So those are interesting numbers. I suppose the people participating in this seminar would be the ones who understand the significance of it to their business but I find that pleasing because it is a very significant arrangement ... people paying attention to it.

Guest Speaker - Patrick Fair (Patrick Fair Associates): How's that?

Webinar Host - Ian Gibson (DSPANZ): Yeah that's much better. But still it's interesting 25% still no, so. There's still people out there that would benefit from it.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): Alright. So let's proceed then to talk about the proposed reforms.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): First big feature is that the impact of those requirements just mentioned are going to be expanded to cover communications, data storage and processing, defence, energy's already in there, but financial markets and services, food and grocery, healthcare. So these sectors, and if you are in those sectors and you have a relevant asset, then you'll have a Positive Security Obligation but only if the Department decides that the rules will apply to you once you're identified.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): There are two tiers of requirements. First you can be a Critical Infrastructure Asset and second you could be a System of National Significance which is a Critical Infrastructure asset which has a relationship with other Critical Infrastructure assets such as interdependency and you get declared by the Minister if you're to be a System of National Significance.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's a CIA? Well, you have to be related to the sector but the Act then defines that and essentially either the Act defines what you are or you are described in some rules to be made yet. And in some cases, and you'll see this in the consultation, the Department is proposing to just go ahead with what the Act says.

So you'll see this is very aggressive. For the telecommunications sector it's any telecommunication network operated by a carrier which is all of them and used to supply a carriage service, also all of them. And for anybody serving a carrier, it's anyone who's a carriage service provider, reselling carriage their network and their assets used in connection and supply.

For critical data storage and processing, the definition is quite long but I'd summarise it like this: if you supply to a state or federal government or you supply to a Critical Infrastructure entity

and your supply relates to business critical data, you would be a regulated critical infrastructure asset or you have one and then as the controlling entity, you'd be regulated.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's business critical data and that definition? Well it's quite aggressive. Essentially it's personal information within the meaning of the Privacy Act relating to 20,000 individuals or any information related to the Critical Infrastructure asset including research and development, systems needed to operate, information needed to operate, information relating to risk management or business continuity. So that's pretty broad.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): Now as I said, the regulation depends on the rules that are made and how it's applied and this is the thing the Parliamentary Joint Committee on Intelligence and Security has said is just too vague and they want it to wait until the consultation is over before passing the Act. But remember, they're proposing to pass it so that doesn't mean that this material isn't going to be relevant.

The other thing to say is that the power of the Minister to prescribe additional assets is not removed and also that the definition - national security business - uses Critical Infrastructure assets in the foreign investment review board definitions and since the 1st of January, any asset in Australia can be called in as to foreign ownership and so you're caught within this web.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So, who's responsible if you have one of these assets? Well it depends on the sector and it's specific to the sector. Where they haven't got a regulated owner because of the way the sector is set up, then it can be prescribed in the rules but it's effectively whoever controls the asset.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): You get some additional obligations a part from those ones I mentioned - reporting, ownership and operational information. You have to have a risk management program, you have to do mandatory reporting of cyber incidents and you need to provide the existing ownership and operator information.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's a risk management program? Well it applies to you as an entity. It means you have to identify each hazard which could have a relevant impact on the asset. You have to prescribe how you're going to minimise or eliminate that risk and then how you're going to mitigate the impact if the hazard occurs. The consultation on these rules has started. There's a web page up at Home Affairs which says when various industries will be dealt with. Gas, electricity, water and data storage and processing have already commenced and I think the initial stage, at least, has concluded.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): You also have to do reporting. You have to file with the regulator at the end of each year how your risk management program went and identifying hazards that occured and how your plan worked dealing with them and whether or not you've updated it appropriately and that's got to be signed off at board level. Quite a serious obligation.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): You also have mandatory incident reporting. You have two levels. If it has a significant relevant impact, you've got 12 hours to let Home Affairs know. And if it's got a relevant impact, you've got 72 hours to let Home Affairs know. There was some pushback from industry about these short times but Parliamentary Joint Committee on Intelligence and Security said "oh it's just a contact you know, you can formalise the detail later. You just have to let them know." So probably okay.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's a relevant impact? Well it's quite a low threshold. Anything that has an impact on the availability, integrity, reliability of the asset or any of the confidentiality of information about the asset is a relevant impact.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So that begs the question - what's a significant relevant impact? And that's not defined in the Act but, if you go to the Explanatory Memorandum, it says it will vary between the sectors, it will be up to you but we think it will probably mean that it affects the functioning of the asset. Which doesn't tell you anything because of course that *(switches back to relevant impact slide)* affects the functioning of the asset. But it will also affect your ability to deliver the intended services. So it's kind of interesting to have a short time, potential penalty, but the threshold is determined by you in relation to the 12 hours in any case.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what's a System of National Significance (SoNS)? As I mentioned, it's something where there's interdependency. It gets declared by the Minister having regard to various matters. You have to be consulted before you can be declared a System of National Significance...

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): ... but if you are, then you pick up some additional obligations. You have to do incident response planning. So remember I just mentioned risk management, having a risk management program, well this is an additional program focusing on incident response. On 30 days notice, you can be required to participate in a cyber exercise. And you can be made to undertake a vulnerability assessment. And you can be made to do event-based reporting to the Department. And you can be made to have systems software installed on your system for the purpose of monitoring. So you really can have the tentacles of government firmly inserted into every nook and cranny in order to ensure that the Department is happy with the way that you maintain your security.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): What's a cyber security exercise? Well it's designed to test your ability, preparedness to respond appropriately and to mitigate relevant impacts of an incident. You have to comply with them as specified in rules to be made and there might be people from the ASD or somewhere else observing what happens. You have to do your own evaluation but if they don't like the evaluation you file, the Department can make you have an external report evaluation prepared and delivered.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): Then there are some much more aggressive powers to respond to serious cyber incidents and these are the ones that the Parliamentary Committee are saying ought to be passed now where the Minister can authorise the Secretary to gather information or take action or even intervene in order to protect a national security asset in the case of an emergency. These powers are quite onerous but there is a reasonable threshold for their exercise. There needs to be a threat to the economic wellbeing, safety and security of Australia. So quite a high threshold and they're also a bit analogous to the powers we've seen the Health Minister use in the pandemic where the State Ministers and the Federal Minister suddenly had discretion to pretty much write law immediately to address the pandemic. So similar sort of approach being put into law here.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): As I said, the threshold for these new powers is quite aggressive. The third dot point there is the one that gets me that material risk of serious prejudice to social or economic stability, defence of Australia or national security.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So that's what the Bill says right but in the meantime, the Department's gone away and had a consultation regarding those questions of coverage. What should we be prescribing this extends to and how should we change what the Act says about the very broad potential coverage and perhaps narrow it down.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So this paper closed on the 14th of May, it went out in April, and the submissions haven't been published and there hasn't been an outcome. The Department says that they are thinking and reviewing.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): But what the paper says is that of the various sectors here, there are these listed described assets in the Act. So I've listed the assets described in the Act under each sector and the ones in blue are going to be defined in rules and the ones in red the paper says will be taken as is. So notice that. Data storage and processing - taken as is and telecommunications - taken as is. But financial markets and services are all going to be defined.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So we'll just have a quick look at those sectors, we don;t have time to do them all. So as I mentioned, for telco, it's proposed to be all networks used to supply carriage services and any other asset used in connection with a carriage service by a carriage service provider. Which is everybody, essentially.

And for data storage - any storage or processing provider that wholly or primarily provides data storage or processing to government or an entity established by a government or to an end user that is a responsible entity for critical infrastructure asset and the service is related to business-critical data, the definition I looked at before. Now it would be amazing to me if that data storage and processing asset survives because as you can see, it's the wrong way around right. If you happen to be a big provider and you've got 100% of the Department's data, you don't get caught because you're not wholly or primarily providing your service to that particular department. Whereas if you're a tiny provider and you're doing something for the Department which is a very small percentage of what they're doing, you might be wholly or primarily

providing the service and you'll be Critical Infrastructure even though to them this data is only a small part of what they do. So I do think they need to rework that but the process for that seems to have gone quiet.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): Also in the finance sector, here are some definitions which were prescribed in the rules just in summary. So for a financial market infrastructure asset, it's the licenced operator of a financial market. For banking it's an authorised deposit-taking institution. For insurance it's focusing on health insurance as prescribed by the rules. And for superannuation it's prescribed in the rules as registrable superannuation entity and there are criteria for that and financial thresholds set out in the discussion paper.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So, as I mentioned, there's that consultation over coverage but then there's another consultation regarding rule making and they've started to make some rules for these various sectors.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): And it started on the 29th of June. At the time of writing the slides, there are only three sectors that had started and I think have finished. But you'll see there's a full timetable up on Home Affairs regarding these now.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So what the rules do, and they seem to follow a template, is describe hazards that your risk management program must deal with and requirements that your risk management program must state you will abide by.

So the first one is cyber security hazards and depending on the sector, various standards and industry cyber security rules are prescribed. Some cases you can pick either sort of an ISO or a NIST. For energy they've gone with the energy industry standards.

And then for personnel, basically everybody's going to be required to do background checks which really does sort of say well wait a second, we need to know exactly what these assets are that are covered because we can't have everybody touching our network getting background checked. You know there are some jobs that aren't just that important.

Then supply chain hazards, physical hazards, natural hazards and material risks including ones that are specific to your particular industry. So for example in data storage and processing, they've prescribed ransomware and malware as material risks that were unique.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So as I've said these rules have to be switched on and when I looked at the rules that are being published, I noticed that they weren't switching anything on. The draft rules that have been consulted on just say this is what your risk management plan has to have in it. So I wrote to the Department and I said are you telling me that you're not actually going to apply this incident notification, this annual reporting, the positive security obligations and they wrote back and said this.

I just thought I'd quote it to you because it gives you a feel for where their mind is. So the rules as to turning on your asset register, your risk management program and your cyber risk reporting obligations will be specific to the sector. So they aren't telling anybody, even now, what's going to apply to you. The Department intends to make this clear on the face of the legislative instrument i.e. not the rules and so we haven't seen that instrument yet. And at this time, they intend to turn on cyber risk reporting obligations for all Critical Infrastructure sectors. So do they really mean that or do they mean assets, I think they mean sectors. And the asset risk register and risk management obligations will be turned on for a majority of sectors. So even with the consultation that's been happening, we're not getting an indication of what the final outcome will be, which tells you why and with all credit to them, the Parliamentary Joint Committee on Intelligence and Security said this isn't good enough, the Department needs to tell us what law they're making and then we'll recommend it be passed by parliament.

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): So just concluding. Issues open for resolution. Can the regime be restricted to only genuinely critical assets? Will it be possible to isolate assets covered from those outside scope or are we going to get something like that significant test where you decide yourself? And will it be possible to manage the application of standards, risk management, personnel requirements for the subset that has been identified?

Slide change

Guest Speaker - Patrick Fair (Patrick Fair Associates): Changes that seem likely. You're going to have this risk management program if you're of significant size. You're going to have a cyber incident reporting regime it seems that's going to be made law even on the PJCIS recommendations. If you're doing your risk management, you're probably going to have the annual reporting regime. And, if you look like you're key or you could be declared a System of National Significance and then you're going to have these additional obligations.

So a bit of a cook's tour in a short time but I hope that gives you a feel for what's in there and Ian I believe we're going to have some more questionnaires and then some questions.

Webinar Host - Ian Gibson (DSPANZ): Just to remind everyone, put your questions into the chat. We do have one more poll and so why don't we do the poll and then I think we can use the rest of our time for the questions.

So the first question there is do you think this could apply to you? The second question is do you think the requirements are reasonable considering the data you're managing? And the third is will these rules make you take additional steps to secure your information?

Whilst that's going on Patrick, I did wonder when you spoke about the relevant impact and you mentioned about the notification period within 12 hours etcetera, so when you have an outage, which is one of the criteria, it's not always clear when you have the outage what's the cause. So it did occur to me, you could end up with this situation where virtually any outage that goes for more than 12 hours, you have to report just because you may not know at that time whether that's actually a cyber incident or not.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Absolutely. It's a bit like the way the GDPR works where they sort of say that you have to notify on 72 hours in the GDPR but the idea is you have a continuous notification obligation. So you start by saying what you know and then you keep saying it. Whereas it's sort of in contrast with the mandatory data breach obligation in the Privacy Act where there are certain things that you need to notify and in fact, that list of things you must notify, can create a barrier to when you notify because "soon as practicable" but you know you have to tell them these things. So if you don't know those things, you could argue well it wasn't practicable to notify. So we don't have that sort of scope here. The fact of the incident gives rise to a duty to tell and then you keep informed after that.

Webinar Host - Ian Gibson (DSPANZ): Well in a former life I worked for a service provider that would probably be caught by this legislation and when you have an incident, one of the issues you have is there's so many different people that you've got to report to for different reasons, it can sometimes be overwhelming particularly for a small firm to know who do I need to report what to and when. And this sort of appreciates *inaudible* but it sort of adds to that unfortunately.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Yeah and I think that's right.

Webinar Host - Ian Gibson (DSPANZ): I think we've got our responses here. So the first question there you'll see 75% thought it would apply to them and given my knowledge of the industry and the members, I think that's probably about right.

Do you think the requirements are reasonable considering the data you're managing?

Guest Speaker - Patrick Fair (Patrick Fair Associates): Well there you go. That's encouraging. I'm pleased to hear that.

Webinar Host - Ian Gibson (DSPANZ): So it would appear that we're heading in the right direction.

Will these rules make you take additional steps to securing your information? 63% said yes.

Guest Speaker - Patrick Fair (Patrick Fair Associates): There you go.

Webinar Host - Ian Gibson (DSPANZ): Given your role and you obviously spend a lot of time in this area, do those results surprise you or meet your expectations?

Guest Speaker - Patrick Fair (Patrick Fair Associates): They kind of do. I must say my reaction to the whole scheme is a little cynical, you know. I remember the Chief Justice of New South Wales, as he then was Murray Gleeson, giving a talk one year at a dinner where he talked about governments having unfunded mandates and how they love to try and earn political capital by legislating and imposing requirements on people particularly if it doesn't require the government to make any expenditure and we've got a great example of that here where a little bit of beefing up down there at Home Affairs and the huge impact on the economy. It's sort of like the anti-repeal red tape day that Tony Abbott had years ago. We've got the opposite going on here. My approach is they haven't really put out significant authoritative stats which are showing a degree of attack, the need for the remediation and also, we're solving the same problem a number of ways. There's already a regulatory regime addressing security called the TSSR for telcos and there's one for energy already. And so they've found a new set of requirements which address the same problem in a different way and legislating those as well so we're getting multiple regulatory schemes focused at the same issue.

That said, the feedback I get from industry and participants is happy to play ball, do want more leverage with their governance bodies to spend money on better cyber security and better controls. So I think that's good. And also, my approach to reading the rules and to be fair also I think in a way the approach that the Parliamentary Joint Committee took was to read what is put in the legislation quite literally. And when you see something like telecommunications network operated by a carrier as a Critical Infrastructure asset, well you read that as every line, every base station, every transponder and so on. But people are experienced dealing with the Department say no, no, no when you see the legislation talking about the network, the Critical Infrastructure that's being described is anything that can bring down the network. So not every part of the network, piece at a time, but anything that's critical to the network as a whole. And when you read the legislation with that kind of mindset, you do see a much narrower set of Critical Infrastructure assets and a more manageable framework.

The problem is that that's not coming across in the way the legislation is drafted. It looks like a literal requirement to have background checks and risk management reporting done on every line from the corner fibre to your house.

Webinar Host - Ian Gibson (DSPANZ): The obligations seem very clear but one of the audience has made the observation that the reasonableness of the requirements are somewhat driven by the degree of ambiguity or lack of ambiguity with their application. So if it's very clear about the application, then that's much easier to make an assessment about the reasonableness of the requirements. Given the ambiguity, then it's hard to sort of make that assessment. But I think what you're sort of alluding to is people are filing that vacuum created by the ambiguity and choosing an interpretation that makes the requirements sort of seem more reasonable rather than it necessarily being the way it should be.

Guest Speaker - Patrick Fair (Patrick Fair Associates): And there's a kind of consistency in that Home Affairs say that, when challenged, oh don't read it like that but I find that infuriating. I mean the number of times we've pointed out something appallingly aggressive in the encryption bill to them and they said oh yeah but we'd never do that. So the law is suddenly whatever you read it to be. I don't think that's a good approach.

Webinar Host - Ian Gibson (DSPANZ): I noticed in the press last week because there's aspects where, in the consultation, Home Affairs went out and sort of said should the codes be mandatory or should they be voluntary. Do they want them industry co-designed or do you want us to come up with them. And the answer in the press last week was no we don't want them compulsory, yes we do want to be co-designed. That actually is in stark contrast with some of the associations. For example, I know our own, we sort of said we think there's a strong case for making the codes compulsory but only on the basis that they're co-designed.

Guest Speaker - Patrick Fair (Patrick Fair Associates): Yeah. I mean I'd say this about this. I produced a document that I'm calling the unofficial rules because there's clearly a template that the Department's using and it's not shared with anybody and you can sort of, if you go across the four published sets of rules and bring them together you come up with a standard document.

And one of the other comments in that correspondence I got from the Department the other day was that the rules that they've been sending haven't been legalled. They're just "policy thoughts" which are being shared and workshopped. And the idea is to go out and say this is what we think will roughly be covered and put that out in a loose paper and then we're going to actually see some rules later. I suppose I can see why somebody would think that's an attractive process but from a public affairs point of view, it's a little bit, it's double handling. From a public affairs point of view, you always look at the literal terms of proposed law or rule, work out what you're getting and what you're not getting and that matters a great deal. So to be getting

something broadly stated and then getting something else tightened up, you're not making progress. You're taking a backwards step with that tightened up version.

Webinar Host - Ian Gibson (DSPANZ): Now, I'm conscious of the time. So perhaps, there is one last question I did want to ask. Given the results of the poll, which clearly indicate people think that this could apply to them that result seems quite overwhelming, is there any advice that you'd give an organisation in terms of what you think they should be doing now to prepare themselves for what might eventuate?

Guest Speaker - Patrick Fair (Patrick Fair Associates): Well the first thing is that Home Affairs is saying that if you have existing rules and programs, they'll be included. They'll satisfy the tests if they do what the Act requires. So I think the first thing to do is to sort of look at what you've got already and try and identify the gaps because that's where the work has to be done.

The second thing is I think it would, I'm hoping that all relevant industry associations and participants are carefully looking at the rules being promulgated and saying how can I propose a change which might reduce the duplication. I've already got a regulatory scheme that deals with this, it achieves a result by a different means but you really want the outcome, you don't need the rules. And therefore for our sector, we say to Home Affairs, don't impose the cyber security rules, we've already got this regulatory framework. Or, do impose this and try to bring it down to something better.

Also some of the feedback in the consultations are that the standards that are being offered, particularly that standard on background checking is a bit old and inappropriate. And those working in the space, now is your chance to get in and say look don't give us that. If we've already got a practice which meets your needs, we don't need you to make us do it another way.

Webinar Host - Ian Gibson (DSPANZ): No that's great and I think that's a great note to finish on. We are just over time so I would like to thank everyone for their attendance. I'd also like to thank our sponsor SuperChoice for making Webinar Week available and I'd also like to thank you Patrick for making your time available. Also just to remind the audience, don't forget to join us tomorrow. We have session three in the morning with the ABS on their directions in digitising business reporting at 11am. And just to remind everyone that this session has been recorded and it will be made available to attendees and on the DSPANZ website over the coming weeks. Any other follow up questions can be sent to hello@dspanz.org. Otherwise, thanks everyone and thanks a lot Patrick.

Guest Speaker - Patrick Fair (Patrick Fair Associates): My great pleasure. Thanks everyone. Bye Ian.