



3 October 2023

█  
████████████████████

Ref: OIA-2023/24-0059

Dear █

**Official Information Act request relating to Cyber Security Advisory Committee (CSAC) and Single Front Door (SFD)**

Thank you for your Official Information Act 1982 (the Act) request received on 27 July 2023. You requested:

- 1. The list of potential panel members for the CSAC, and the Ministers who appointed the selected panel members to the CSAC*
- 2. Copies of the Terms of Reference for the CSAC, including the four workstreams*
- 3. CSAC meeting agendas from 20 December 2021 to the current date*
- 4. DPMC issues paper from the inaugural workshop, referred to on page 13 of the CSAC Report, 24 March 2022*
- 5. Customer orientation study questions, participants, responses, and findings (March 2022)*
- 6. Final report on workstream 4 (22 May 2022)*
- 7. Supplementary issues paper (28 June 2022)*
- 8. Feedback on June Cabinet paper "Cyber Security - Strengthening resilience in the wider economy" (26 July 2022), and the cabinet paper itself, if not proactively released*
- 9. List of agencies consulted on the SFD draft (approximately September 2022), dates and timeframes for consultation, and responses*
- 10. The further report prepared in October 2022 referred to in the answer of PQ 12199 (2023)*
- 11. The SFD recommendations to Ministers (15 October 2022) [if not the same as above]*
- 12. Official correspondence with CSAC, Ministers, and / or other agencies related to CSAC and / or SFD*
- 13. Conflicts of Interest declared by CSAC committee members*
- 14. Information on consultations undertaken by or on behalf of CSAC, or about SFD, if any, including parties consulted, dates and timeframes for consultation, and responses*

15. *Date of dissolution of the CSAC*

16. *Budget appropriations and / or expenditures of the CSAC*

*n.b.: If responses to consultations are to be withheld under the OIA, please provide a numerical summary of any submissions: (for / against / neutral), (individual / organisation), (counts). If a numerical summary in this approximate format is not held, please seek clarification and advise what is held or is able to be created.*

On 24 August 2023, I responded to the following questions of your request – 1, 2, 4, 6, 7, 8, 10, 11, 15, and 16. In my response, I advised that some information would take longer to prepare. I am now in a position to respond to your outstanding questions. Thank you for your patience as we processed your request.

The responses to questions 3, 5, 9, 12, 13, and 14 are as follows.

### **3. CSAC meeting agendas from 20 December 2021 to the current date**

Please find enclosed the agendas for the Cyber Security Advisory Committee (CSAC) for the period of 20 December 2021 – 28 September 2022, subject to information being withheld as noted. The relevant grounds under which information has been withheld are as follows:

- section 9(2)(a), to protect the privacy of individuals
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials
- section 9(2)(k), to prevent disclosure or use for improper gain or advantage.

Please note that there is an administrative error in the CSAC meeting agenda for 13 September 2022. Where the agenda refers to Liz McPherson, Chief Executive from the Office of the Privacy Commissioner, that should be Liz MacPherson, Deputy Privacy Commissioner.

In my response to you on 24 August 2023, you were referred to an earlier response to a request for CSAC agendas and minutes which included a typographical error. The grounds relating to the withholding of CSAC meeting minutes, 9(2)(b)(i) and 9(2)(b)(ii), should have been 9(2)(ba)(i) and 9(2)(ba)(ii). The descriptions on why the material is withheld in the earlier response are correct and the error is contained to the redaction code only.

### **5. Customer orientation study questions, participants, responses, and findings (March 2022)**

I can advise that the study questions, participants, and responses are withheld in full under section 9(2)(ba)(i), to protect the supply of similar information in the future, where information was provided in confidence.

As referred to in our earlier response to you of 24 August 2023, the findings are publicly available, here:

[New Zealand Cabinet Cyber Security Advisory Committee Report back on Workstreams 1/2/3 - July 2023 - Department of the Prime Minister and Cabinet \(dpmc.govt.nz\)](https://www.dpmc.govt.nz/new-zealand-cabinet-cyber-security-advisory-committee-report-back-on-workstreams-1/2/3-july-2023-department-of-the-prime-minister-and-cabinet-dpmc.govt.nz)

**9. List of agencies consulted on the SFD draft (approximately September 2022), dates and timeframes for consultation, and responses**

I can advise that the list of agencies consulted is withheld in full under section 9(2)(ba)(i), to protect the supply of similar information in the future, where information was provided in confidence.

**12. Official correspondence with CSAC, Ministers, and / or other agencies related to CSAC and / or SFD**

Please find enclosed copies of official correspondence from the Minister for the Digital Economy and Communications to CSAC members, subject to information being withheld as noted. The relevant grounds under which information has been withheld are:

- section 9(2)(a), to protect the privacy of individuals
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials.

Please note, Mandy Simpson left the Cyber Security Advisory committee mid-term and was not replaced. Therefore, there is no extension or conclusion letter for Mandy Simpson.

Furthermore, the appointment letters included identical attachments to all committee members. As such, we have included one copy of the attachments in the enclosure.

**13. Conflicts of Interest declared by CSAC committee members**

Please find enclosed copies of the Conflict-of-Interest forms for members of the CSAC, subject to information being withheld as noted. The relevant grounds under which information has been withheld are:

- section 9(2)(a), to protect the privacy of individuals.

**14. Information on consultations undertaken by or on behalf of CSAC, or about SFD, if any, including parties consulted, dates and timeframes for consultation, and responses**

This information is withheld in full under section 9(2)(ba)(i), to protect the supply of similar information in the future, where information was provided in confidence.

In making my decision, I have considered the public interest considerations in section 9(1) of the Act. No public interest has been identified that would be sufficient to override the reasons for withholding that information. You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act. This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely



Tony Lynch  
**Deputy Chief Executive**

## Cyber Security Advisory Committee - establishment meeting agenda

<b>Date/Time</b>	20 December, 3.30pm – 6.00pm
<b>Venue</b>	MS Teams
<b>Chair</b>	Mike O'Donnell (MOD)
<b>CSAC Members</b> <i>(to be confirmed by APH on 15 December)</i>	Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Hamish Rumbold Mandy Simpson
<b>Ministers</b>	Hon Dr David Clark, Minister for the Digital Economy and Communications Hon Andrew Little, Minister Responsible for the Government Communications Security Bureau
<b>Participating officials</b>	Governance group senior officials (DPMC, MBIE, DIA, GCSB, Police) CSAC Secretariat
<b>Apologies</b>	

Item	Topic	Time	Lead
1	Welcome and apologies (5 mins)	3.30pm	MOD/DPMC
2	Round the table self intro of CSAC members and key officials (10 mins)	3.35pm	MOD/CSAC/ DPMC
3	Overview from officials on current context for cyber security in Aotearoa and snapshot of government work relevant to the CSAC TOR (40 mins).	3.45pm	Senior officials
4	Initial thoughts on sizing and delivering the four TOR outcomes across the next six months - specifically providing advice on: <ul style="list-style-type: none"> <li>- lifting private sector CS capability in NZ</li> <li>- recommending a scalable cyber security framework for NZ</li> <li>- assessing customer orientation of Govt agencies</li> <li>- establishing a permanent cyber security collaboration forum</li> </ul>	4.25 pm	CSAC Members
5	Discussion with Ministers Clark and Little on initial thoughts/next steps (45 mins) <i>Ministers Clark and Little are scheduled to attend from 5.00pm.</i>	5.00pm	MOD/DPMC

6	Next steps, covering (10 mins): <ul style="list-style-type: none"><li>- drafting of workplan including working cadence</li><li>- meeting calendar</li><li>- engagement with Ministers/officials</li><li>- admin/secretariat support of CSAC</li></ul>	5.45pm	CSAC/DPMC
7	Any other business + close (5 mins)	5.55pm	All

## Cyber Security Advisory Committee – Agenda 13 Jan '22

<b>Date/Time</b>	13 January, 10am – 2 pm
<b>Venue</b>	MBIE Stout St Wellington
<b>CSAC Attendees</b>	Mike O'Donnell (MOD) Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Mandy Simpson Hamish Rumbold (via Video)
<b>Officials attending</b>	s9(2)(a)

Item	Topic	Time	Lead
1	Welcome and grab coffee	10am	All
2	Committee only time	10:05	MOD
3	Bucketing up the CSAC terms of reference and allocating work across CSAC members for delivering on TOR – splitting 8 members across 3 workplans.	10:15	MOD + Members
4	Scoping/brainstorming the workplan for CSAC advice on lifting private sector CS capability in NZ.	10:30	All members
5	s 9(2)(g)(i)	11:15	All
	Bio Break – Grab MBIE Sandwiches	Noon	All
6	Getting ready to proceed with customer orientation survey – approving final draft of questions and commencing surveying.	12:15	All
7	Timing of recommendations for establishing a permanent cyber security collaboration forum.	1:00	All
8	Fleshing out the timeline for the next six months and timing of next meeting	1:30	All
9	Any other business	1:50	All
10	Meeting finish – head home	2pm	All

# Cyber Security Advisory Committee – Agenda 28 Jan '22

<b>Date/Time</b>	28 January, 2:00pm – 4:15pm
<b>Venue</b>	Microsoft Teams Meeting (Virtual)
<b>CSAC Attendees</b>	<p>Mike O'Donnell (MOD)                  Sheridan Broadbent                  Vanessa Clark                  Jon Duffy                  Steve Honiss                  Victoria MacLennan                  Mandy Simpson                  Hamish Rumbold</p>
<b>Officials attending</b>	<p>s9(2)(a) [redacted]                  s9(2)(a) [redacted]</p>

Item	Topic	Time	Lead
1	Committee only time	2:00pm	
2	CSAC Data Collection - Procedure around confidentiality and data	2:10pm	s9(2)(a) [redacted]
3	Customer Orientation Survey update and discussion with group	2:30pm	MOD + Members
4	Capability and resilience update and discussion with group	2:50pm	Mandy + Members
5	Bio Break	3:10pm	
	Cyber Security Framework update and discussion with group	3:20pm	Sheridan + Members
6	General business	3:40pm	
7	Looking ahead	4:00pm	
8	Wrap	4:15pm	

## Cyber Security Advisory Committee – Agenda 16 Feb ‘22

<b>Date/Time</b>	16 February, 11:30am – 3:00pm
<b>Venue</b>	Room G.05, 15 Stout Street / Microsoft Teams Meeting
<b>CSAC Attendees</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent (Virtual) Vanessa Clark (Virtual) Jon Duffy (Virtual) Steve Honiss Victoria MacLennan (Virtual) Mandy Simpson (Virtual) Hamish Rumbold (Virtual)
<b>Secretariat &amp; Support</b>	s9(2)(a) [REDACTED] s9(2)(a) [REDACTED] s9(2)(a) [REDACTED]
<b>Officials attending</b>	Ministers only

Item	Topic	Time	Lead
1	Committee only time	11:30am	Chair
2	Workstream findings & initial recommendations	11:45am	MOD/ Sheridan/Vic
3	Ministers Little and Clark – Update on progress	12:30pm	Chair
4	Working Lunch and Workstream findings & initial recommendations (cont.)	1:00pm	All CSAC
5	Format – ‘do we need a Preamble Paper’?	1:50	Chair
6	Wrap up and next steps around group critique + completing survey	2:05	Chair
7	Guest Speaker – Liz MacPherson from OPC (Virtual)	2:15 / 2:45	Liz



## Cyber Security Advisory Committee – Agenda

<b>Date/Time</b>	2 <sup>nd</sup> March, 11:00am – 2:00pm
<b>Venue</b>	Virtual - Microsoft Teams Meeting
<b>CSAC Members and Attendees</b>	<ul style="list-style-type: none"> <li>• Mike O'Donnell (MOD) – Chair</li> <li>• Sheridan Broadbent</li> <li>• Vanessa Clark</li> <li>• Jon Duffy</li> <li>• Steve Honiss</li> <li>• Victoria MacLennan</li> <li>• Hamish Rumbold</li> <li>• Mandy Simpson</li> </ul>
<b>Secretariat &amp; Support</b>	<ul style="list-style-type: none"> <li>• s9(2)(a) [REDACTED], Programme Lead (MBIE)</li> <li>• s9(2)(a) [REDACTED], Senior Policy Advisor (DPMC)</li> <li>• s9(2)(a) [REDACTED], Programme Coordinator (MBIE)</li> </ul>
<b>Officials attending</b>	N/A

Item	Topic	Time	Lead
1	Committee only time	11:00am	Chair
2	Workstream 1 (capability) – Review and Recommendations	11:15 am	Mandy
3	Bio Break / grab food	12:00pm	Chair
4	Workstream 2 (framework) – Review and Recommendations	12:15pm	Sheridan
5	Workstream 3 (customer) – Survey progress & Review and Recommendations	1:00pm	MOD
6	Preamble Paper - Review	1:45	Chair
7	Wrap up and next steps	1:55	Chair

# Cyber Security Advisory Committee – Agenda

<b>Date/Time</b>	15 <sup>th</sup> March, 1:30pm – 3:30pm
<b>Venue</b>	Virtual - Microsoft Teams Meeting
<b>CSAC Members and Attendees</b>	<ul style="list-style-type: none"> <li>• Mike O'Donnell (MOD) – Chair</li> <li>• Sheridan Broadbent</li> <li>• Vanessa Clark</li> <li>• Jon Duffy</li> <li>• Steve Honiss</li> <li>• Victoria MacLennan</li> <li>• Hamish Rumbold</li> </ul>
<b>Secretariat &amp; Support</b>	<ul style="list-style-type: none"> <li>• s9(2)(a) [redacted], Programme Lead (MBIE)</li> <li>• s9(2)(a) [redacted], Senior Policy Advisor (DPMC)</li> <li>• s9(2)(a) [redacted], Programme Coordinator (MBIE)</li> <li>• s 9(2)(a) [redacted], The Research Company (TRA), 2:00 to 2:30 pm</li> </ul>
<b>Apologies</b>	Mandy Simpson Jon Duffy

Item	Topic	Time	Lead
1	Committee only time	1:30pm	Chair
	Final review of Report	1:40 pm	Chair/All
	Survey – The Research Company – Summary of findings	2:00pm	s 9(2)(a) [redacted] (TRA)
2	Final review of Report (Cont.)	2:30pm	Chair / All
3	Agreement of Recommendations	3:15pm	Chair / All
7	Wrap up and next steps	3:25pm	Chair

# Cyber Security Advisory Committee – Agenda

<b>Date/Time</b>	11 <sup>th</sup> April, 11:00am – 1:00pm ( <i>note the shortened time</i> )
<b>Venue</b>	MBIE Building Stout Street Wellington   MS Team Meeting
<b>CSAC Members and Attendees</b>	<ul style="list-style-type: none"> <li>• Mike O'Donnell (MOD) – Chair</li> <li>• Sheridan Broadbent</li> <li>• Vanessa Clark</li> <li>• Jon Duffy</li> <li>• Steve Honiss</li> <li>• Victoria MacLennan</li> <li>• Hamish Rumbold</li> <li>• Mandy Simpson</li> </ul>
<b>Secretariat &amp; Support</b>	<ul style="list-style-type: none"> <li>• 9(2)(a) [redacted], Programme Lead (MBIE)</li> <li>• 9(2)(a) [redacted], Senior Policy Advisor (DPMC)</li> <li>• 9(2)(a) [redacted], Programme Coordinator (MBIE)</li> </ul>
<b>Apologies</b>	N/A

Item	Topic	Time	Lead
1	Committee only time	11:00 am	Chair
2	Housekeeping – update on various activities	11:10 am	Chair
3	CSAC members views/approach on collaboration forum (5-10 minutes each)	11:20 pm	Chair / All
4	Bio break / Lunch	12:00 pm	All
5	Cont. Approach to collaboration forum & summary	12:15 pm	Chair / All
6	Wrap up and next steps	12:50 pm	Chair

Reference email for agenda item 3 & 5

Out of scope



## Cyber Security Advisory Committee – Agenda 2<sup>nd</sup> May '22

<b>Date/Time</b>	2 <sup>nd</sup> May, 11:00am – 1:00pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.3
<b>CSAC Attendees</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Hamish Rumbold
<b>Secretariat &amp; Support</b>	s9(2)(a) [REDACTED] s9(2)(a) [REDACTED] s9(2)(a) [REDACTED]
<b>Apologies</b>	Sheridan Broadbent

Item	Topic	Time	Lead
1	Committee only time	11:00am	Chair
2	Collaboration Forum – Review/feedback of draft paper	11:10am	Chair/All
3	Bio break / Lunch	12:00pm	All
5	Potential non-TOR Cyber issues for Ministers	12:15pm	Chair/All
6	Wrap up and next steps	12:45pm	Chair
7	Finish	1:00	

# Cyber Security Advisory Committee – Agenda 1<sup>st</sup> June ‘22

<b>Date/Time</b>	1 <sup>st</sup> June, 2:00pm – 4:00pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.14
<b>CSAC Attendees</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Hamish Rumbold
<b>Secretariat &amp; Support</b>	s9(2)(a) [REDACTED] s9(2)(a) [REDACTED] s9(2)(a) [REDACTED]
<b>Apologies</b>	

Item	Topic	Time	Lead
1	Committee only time	2:00	Chair/ members
2	Minister feedback/advice on TOR4 / 'Magnus Opus'	2.10	Chair / All
3	Initial Skeleton/Additional issues/other content of paper	2:25	All
5	Bio break (if needed)	3:00	All
6	Wrap up and next steps + future meetings	3:50	Chair
7	Finish	4:00	Chair
8.	Garage project tap room: 7 Marion Street. Te Aro	5:00	All
	Cinderella – Dinner 278 Willis Street, Te Aro, Wellington	6:30	

# Cyber Security Advisory Committee – Agenda 11<sup>th</sup> July 22

<b>Date/Time</b>	11 <sup>th</sup> July, 10:00 am – 1:00 pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.03
<b>CSAC Attendees</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Hamish Rumbold
<b>Officials</b>	Halia Haddad, Manager, National Cyber Policy Office, DPMC s9(2)(a), Principal Policy Advisor, National Cyber Policy Office, DPMC
<b>Secretariat &amp; Support</b>	s9(2)(a) s9(2)(a) s9(2)(a)
<b>Apologies</b>	Vanessa Clark Hamish Rumbold

Item	Topic	Time	Lead
1	Committee only time	10:00	Chair
2	Overview of Cyber Security – Strengthening resilience in the wider economy' Cabinet paper including: <ul style="list-style-type: none"> <li>swim-lane (relationship) views</li> <li>Outline of additional initiatives referenced in the Cabinet paper</li> </ul>	10.15	Halia/s 9(2)(a)
3	CSAC Feedback and Questions	11:00	All Halia/s 9(2)(a)
5	Lunch /Bio break (if needed)	12:00	All
	CSAC Feedback and Questions (Cont.)	12:15	All Halia/s 9(2)(a)
6	Wrap up and next steps	12:50	Chair
7	Finish	1:00	Chair

## Next Meetings:

- Monday 25 July – Workshop
- Monday 15 August – Workshop
- Monday 29 August – Check in meeting (Online)
- Tuesday 13 September – Check in Meeting (Online)
- Wednesday 28 September – Workshop
- Tuesday 11 October - Workshop

# Cyber Security Advisory Committee – Agenda 25<sup>th</sup> July 22

<b>Date/Time</b>	25 <sup>th</sup> July, 3:00 pm – 5:00 pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.01
<b>CSAC Members</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent (Virtual) Vanessa Clark Jon Duffy Steve Honiss (Virtual) Victoria MacLennan Hamish Rumbold
<b>Officials</b>	Halia Haddad, Manager, National Cyber Policy Office, DPMC s9(2)(a), Principal Policy Advisor, National Cyber Policy Office, DPMC
<b>Secretariat &amp; Support</b>	s9(2)(a) s9(2)(a) s9(2)(a) s9(2)(a) (MBIE Service Design Lead)
<b>Apologies</b>	Hamish Rumbold Vanessa Clark

Item	Topic	Time	Lead
1	Committee only time	3:00	Chair
2	Review CSAC final draft response to Cyber Security in the Broader Economy Cabinet Paper	3.10	Chair/CSAC
3	<p>Single front door</p> <p>1. Review three user cases:</p> <p>i. <u>Jon's Plumbing</u> – hi-jacked credentials to CRM, Xero and Banking – exfiltration and ransom demand to restore access. <i>Jon Duffy.</i></p> <p>ii. <u>Aoraki Wananga College</u> – phishing leading to false invoicing and payment <i>Vic MacLennan.</i></p> <p>iii. <u>Acme Financial Services</u> – DDOS attack with 1 week ransom demand to allow continued customer access. <i>Mystery guest.</i></p> <p>Objective: work through each use-case and how SFD would respond and marshal resources and use this to start shaping up the MVP/Value proposition.</p>	3:30	CSAC with support from Halia s9(2)(a)
5	Wrap up and next steps	4:50	Chair
7	Finish	5:00	

## Next Meetings:

- Monday 15 August – Workshop
- Monday 29 August – Check in meeting (Online)
- Tuesday 13 September – Check in Meeting (Online)
- Wednesday 28 September – Workshop
- Tuesday 11 October - Workshop

## Cyber Security Advisory Committee – Agenda 15<sup>th</sup> August 22

<b>Date/Time</b>	15 <sup>th</sup> August, 11:00 am – 3:00 pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.03 s 9(2)(k)
<b>CSAC Members</b>	<ul style="list-style-type: none"> <li>➤ Mike O'Donnell (MOD) – Chair</li> <li>➤ Sheridan Broadbent</li> <li>➤ Vanessa Clark (Virtual)</li> <li>➤ Jon Duffy</li> <li>➤ Steve Honiss</li> <li>➤ Victoria MacLennan</li> <li>➤ Hamish Rumbold</li> </ul>
<b>Officials</b>	<p><u>Department of Prime Minister and Cabinet</u></p> <ul style="list-style-type: none"> <li>➤ Halia Haddad, Manager, National Cyber Policy Office</li> <li>➤ s 9(2)(a), Principal Policy Advisor, National Cyber Policy Office</li> <li>➤ s 9(2)(a), Principal Policy Advisor, National Cyber Policy Office</li> </ul> <p><u>Government Communications and Security Bureau</u></p> <ul style="list-style-type: none"> <li>➤ Grace Campbell-Macdonald, Director, Regulatory &amp; Advisory, National Cyber Security Centre</li> <li>➤ Lisa Fong, Deputy Director General, National Cyber Security Centre</li> <li>➤ s 9(2)(a), Principal Advisor, Regulatory &amp; Advisory, National Cyber Security Centre</li> <li>➤ s 9(2)(a), Principal Advisor, Regulatory &amp; Advisory, National Cyber Security Centre</li> </ul>
<b>Ministers</b>	Honourable Dr David Clark, Minister of Digital Economy and Communication
<b>Secretariat &amp; Support</b>	<ul style="list-style-type: none"> <li>➤ s 9(2)(a), Programme Lead (MBIE)</li> <li>➤ s 9(2)(a), Senior Policy Advisor (DPMC)</li> <li>➤ s 9(2)(a), Programme Co-ordinator (MBIE)</li> </ul>
<b>Apologies</b>	Sheridan Broadbent

Item	Topic	Time	Lead
1	Committee only time	11:00	Chair
2	Single front door – Use case finalisation, report approach and Q&A	11:25	CSAC/DPMC
3	Working Lunch – cont. item 2	12:00	All
4	Minister Dr David Clark - Update and CSAC Q&A (SFD, Response to Cyber Security in the Broader Economy Cabinet Paper etc)	1:00	Chair / Minister
5	Cyber Framework Overview and Q&A	2:00	CSAC / NCSC
6	Wrap up and next steps	2:50	Chair
7	Finish	3:00	

### Next Meetings:

- Monday 29 August – Check in meeting (Online)
- Tuesday 13 September – Check in Meeting (Online)
- Wednesday 28 September – Workshop
- Tuesday 11 October - Workshop



# Cyber Security Advisory Committee – Agenda 13<sup>th</sup> September 22

<b>Date/Time</b>	13 <sup>th</sup> September, 11:00 am – 12:30 pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.03 s 9(2)(k)
<b>CSAC Members</b>	<ul style="list-style-type: none"> <li>➤ Mike O'Donnell (MOD) – Chair</li> <li>➤ Sheridan Broadbent (In-person)</li> <li>➤ Vanessa Clark (Virtual)</li> <li>➤ Jon Duffy (In-person)</li> <li>➤ Steve Honiss (In-person)</li> <li>➤ Victoria MacLennan (In-person)</li> <li>➤ Hamish Rumbold (Virtual)</li> </ul>
<b>Officials</b>	<p><u>Department of Prime Minister and Cabinet</u></p> <ul style="list-style-type: none"> <li>➤ Dan Eaton, National Cyber Policy Office</li> <li>➤ Tony Lynch, National Cyber Policy Office</li> <li>➤ Halia Haddad, Manager, National Cyber Policy Office</li> <li>➤ s 9(2)(a), Principal Policy Advisor, National Cyber Policy Office</li> <li>➤ s 9(2)(a), Principal Policy Advisor, National Cyber Policy Office</li> </ul> <p><u>Government Communications and Security Bureau</u></p> <ul style="list-style-type: none"> <li>➤ Hamish Beaton, National Cyber Security Centre</li> <li>➤ Lisa Fong, Deputy Director General, National Cyber Security Centre</li> </ul> <p><u>Office of the Privacy Commissioner</u></p> <ul style="list-style-type: none"> <li>➤ Liz McPherson, Chief executive</li> </ul> <p><u>New Zealand Police</u></p> <ul style="list-style-type: none"> <li>➤ Jeremy Wood, Executive Director, Policy and Partnerships</li> <li>➤ Stuart Mills</li> <li>➤ s 9(2)(a)</li> </ul> <p><u>Ministry of Business, Immigration and Employment</u></p> <ul style="list-style-type: none"> <li>➤ Ross van der Schyff, General Manager Business and Consumer</li> <li>➤ Rob Pope, Director, CERT NZ</li> </ul> <p><u>Department of Internal Affairs</u></p> <ul style="list-style-type: none"> <li>➤ Mike West, Acting Deputy Chief Executive, Digital Public Service</li> </ul> <p><u>Netsafe</u></p> <ul style="list-style-type: none"> <li>➤ Sean Lyons, Chief Online Safety Officer</li> <li>➤ Brent Carey, Chief Executive</li> </ul>
<b>Secretariat &amp; Support</b>	<ul style="list-style-type: none"> <li>➤ s 9(2)(a), Programme Lead (MBIE)</li> <li>➤ s 9(2)(a), Senior Policy Advisor (DPMC)</li> <li>➤ s 9(2)(a), Programme Co-ordinator (MBIE)</li> </ul>
<b>Apologies</b>	N/A

Item	Topic	Time	Lead
1	Committee only time	11:00	Chair
2	Single Front Door – Overview of CSAC Recommendations	11:10	Chair / All
3	Wrap up and next steps	12:25	Chair

4	Finish	1:00	
---	--------	------	--

**Next Meetings:**

- Wednesday 28 September – Workshop
- Tuesday 11 October - Workshop

# Cyber Security Advisory Committee – Agenda 28<sup>th</sup> September 22

<b>Date/Time</b>	28 <sup>th</sup> September, 9:00 am – 12:00 pm
<b>Venue</b>	Microsoft Teams Meeting / MBIE Stout G.11
<b>CSAC Members</b>	Mike O'Donnell (MOD) - Chair Sheridan Broadbent Vanessa Clark Jon Duffy Steve Honiss Victoria MacLennan Hamish Rumbold
<b>Officials</b>	s 9(2)(a) [redacted], Principal Policy Advisor, National Cyber Policy Office, DPMC s 9(2)(a) [redacted], Principal Policy Advisor, National Cyber Policy Office, DPMC
<b>Secretariat &amp; Support</b>	s 9(2)(a) [redacted] s 9(2)(a) [redacted] s 9(2)(a) [redacted]
<b>Apologies</b>	Hamish Rumbold

Item	Topic	Time	Lead
1	Committee only time	9:00	Chair
2	Review of single front door recommendations	9:15	CSAC with support from s 9(2)(a) [redacted]
3	Morning Tea / Bio break	10:30	All
4	Feedback on Single front door	10:45	CSAC
5	Wrap up and next steps	11:45	CSAC
6	Finish	12:00	

## Next Meetings:

- October (TBC) - Workshop

## Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Hamish Rumbold

via email to: s 9(2)(a)

Dear Hamish,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Sheridan Broadbent, Vanessa Clark, Jon Duffy, Steve Honiss, Victoria MacLennan and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.



**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Jon Duffy

via email to: s 9(2)(a)

Dear Jon,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Sheridan Broadbent, Vanessa Clark, Steve Honiss, Victoria MacLennan, Hamish Rumbold and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.

A handwritten signature in blue ink, consisting of a stylized 'D' and 'C' intertwined.

**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Mandy Simpson

via email to: s 9(2)(a)

Dear Mandy,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Sheridan Broadbent, Vanessa Clark, Jon Duffy, Steve Honiss, Victoria MacLennan and Hamish Rumbold.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

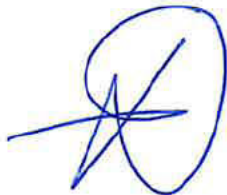
The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.



Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.

A handwritten signature in blue ink, consisting of a large, stylized 'D' with a horizontal line through it, and a vertical line extending upwards from the center of the 'D'.

**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Mike O'Donnell

via email to: s 9(2)(a)

Dear Mike,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as Chair of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

In addition to you, a further 7 CSAC members have been appointed. These are Sheridan Broadbent, Vanessa Clark, Jon Duffy, Steve Honiss, Victoria MacLennan, Hamish Rumbold, and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for the CSAC Chair has been set at NZ\$885 per 8-hour period (a day). The CSAC Chair may spend up to approximately 4 days per month on Committee activities and is expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

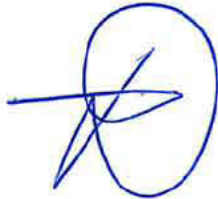
The Code of Conduct for all CSAC members (including the Chair) is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If

you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.

A handwritten signature in blue ink, consisting of a large, stylized 'D' with a horizontal line crossing it, and a vertical line extending downwards from the center of the 'D'.

**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Sheridan Broadbent  
via email to: s 9(2)(a)

Dear Sheridan,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Vanessa Clark, Jon Duffy, Steve Honiss, Victoria MacLennan, Hamish Rumbold and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.

A handwritten signature in blue ink, appearing to be 'D Clark', enclosed within a large, loopy blue circle.

**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Steve Honiss

via email to: s 9(2)(a)

Dear Steve,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Sheridan Broadbent, Vanessa Clark, Jon Duffy, Victoria MacLennan, Hamish Rumbold and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.



**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Vanessa Clark

via email to: s 9(2)(a)

Dear Vanessa,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed: Sheridan Broadbent, Jon Duffy, Steve Honiss, Victoria MacLennan, Hamish Rumbold and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.



Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.



**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



20 December 2021

Victoria MacLennan

via email to: s 9(2)(a)

Dear Victoria,

I am pleased to confirm that Cabinet, on the recommendation of the Appointment and Honours Committee, has appointed you as a member of the Cyber Security Advisory Committee (CSAC). The Committee provides independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society. I look forward to your contribution to this Committee.

I have appointed Mike O'Donnell as Chair of the CSAC. In addition to you, a further six CSAC members have been appointed Sheridan Broadbent, Vanessa Clark, Jon Duffy, Steve Honiss, Hamish Rumbold and Mandy Simpson.

I am writing to set out the terms of your appointment as a member of the CSAC. You are appointed for a term commencing immediately and expiring no later than 15 June 2022. More information on the role of the CSAC and responsibilities of its members can be found in the draft Terms of Reference attached to this letter. We welcome your feedback on the Terms of Reference and expect that amendments of a non-substantive nature can be agreed between me and the CSAC. Substantive amendments will need to be referred to Cabinet for further consideration.

The fees and allowances relating to this appointment are in line with the Cabinet Fees Framework as established by Te Kawa Mataaho Public Service Commission. Payment for CSAC members has been set at NZ\$560 per 8-hour period (a day). CSAC members may spend up to approximately 3 days per month on Committee activities and are expected to attend approximately one meeting per month with me and Minister Little, to be held virtually or as otherwise advised. Should the Ministers wish to convene an in-person meeting, any relevant expenses such as travel and accommodation will be reimbursed. The work of the CSAC will be supported by a Secretariat.

The Code of Conduct for all CSAC members is attached. The Code of Conduct sets out expectations for the general conduct of CSAC members including the management of any conflicts of interest. This is to ensure the CSAC operates in an open and transparent manner and in accordance with the law. Any breach of the Code of Conduct will be reported to the Chair who will determine an appropriate response. All CSAC members are expected to read the Code of Conduct and sign the attached declaration, which confirms their understanding and willingness to comply with it.

Each CSAC member is expected to accept in writing the terms of the appointment, including confirmation of any identified conflicts of interest, and an agreed plan for managing these. If you believe you may have a conflict of interest, please get in touch with the CSAC Secretariat s 9(2)(k) to discuss an appropriate management plan.

All CSAC members are also required to complete an IR330C tax form (attached) and return this to the Secretariat. You will also need to supply a monthly invoice for fees and charges (using the information in the documentation attached), so the Secretariat can arrange payments. For further information please contact s 9(2)(k)

I look forward to working with you to advance New Zealand's cyber security and resilience.



**Hon Dr David Clark**  
Minister for the Digital Economy and Communications

**Attachments:**

- Draft Terms of Reference
- Code of Conduct for CSAC members
- Acceptance of Appointment form
- Code of Conduct Agreement
- Information regarding payments of fees to CSAC Members
- Fees Payment Invoice template
- IR330C form

# **DRAFT TERMS OF REFERENCE FOR THE CYBER SECURITY ADVISORY COMMITTEE (CSAC)**

## **Context**

---

1. Public-private collaboration is a key element in best-practice development and delivery of cyber security initiatives. While the government has a central role in national security and critical events, the private sector develops and deploys most cyber security solutions. A coordinated approach to security, drawing on public and private sector inputs, will provide the best way for us to strengthen New Zealand's overall resilience, reduce duplication, and improve security outcomes for all.
2. New Zealand's Cyber Security Strategy 2019 provides a framework for government-led action and sets New Zealand's direction for cyber security. Amongst its priorities, the Strategy outlines the importance of public and private sector cooperation and articulates the importance of joint leadership.
3. The government is currently considering options to lift the cyber security and resilience of both the public and private sectors in New Zealand. Advice from the private sector on how best to achieve this will be essential in ensuring effective, innovative, and ambitious solutions are considered as part of this work.

## **The purpose and scope of the Cyber Security Advisory Committee**

---

4. The Cyber Security Advisory Committee (CSAC) is convened by the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, to provide independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society.
5. The purpose of the CSAC will be to provide ideas, advice, and options to Ministers and to government agencies on:
  - Lifting the cyber security capability of the private sector and its resilience when under threat;
  - Providing recommendations around a scalable cyber security framework for New Zealand companies and organisations;
  - Providing insight and recommendations around the customer orientation of government agencies working on cyber security matters; and
  - The design and establishment of a permanent public-private collaboration forum on cyber security with the aim of better connecting and harnessing the New Zealand cyber security ecosystem.
6. Out of scope for the CSAC is other work being undertaken across government, such as education, the economy, investment, and trade policies, unless specifically requested by the Minister or unless it has a direct bearing on the areas outlined above.

## **Outputs**

---

7. The CSAC will:
  - Draw on the expertise of the private sector and civil society and international good practice to deliver advice to the Ministers on tackling specific issues within the focus areas outlined above. This could take the form of reports, recommendations, advice, or comment on government papers.
  - As appropriate, work closely with and consider the work of other relevant groups and processes across the public service in providing advice to government (such as the Digital Council for Aotearoa, the Digital Strategy for Aotearoa, and the Data Iwi Leaders Group).
  - Have regard for the Treaty of Waitangi / Te Tiriti o Waitangi when forming their advice to the Minister.
8. The specific deliverables the CSAC will address during its term will be agreed between the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, and the Chair.
9. The Minister may ask for the CSAC to provide specific pieces of ad-hoc advice as issues arise.
10. If the CSAC believes there is an issue of importance that is emerging and not being adequately addressed, the Chair will raise this with the responsible Minister for discussion and consideration.

## **Accountability**

---

11. The Committee is accountable to the Minister for the Digital Economy and Communications for the quality and timeliness of its advice and any reports.

## **How the CSAC will deliver its work**

---

12. The Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, will be responsible for setting the specific deliverables for the CSAC and determining the timeframes for delivery.
13. The CSAC is expected to report to, and meet with, the two Ministers (or their representatives) every month or as agreed. Other communication may also be required in between, particularly with the Chair.
14. The CSAC will also be required to meet with government agencies up to once per month or as agreed, to share ideas, and discuss and offer comment on proposals. Officials will be responsible for further analysis, scoping, and refining of any ideas or options proposed by the CSAC.

## **Membership and appointments**

---

15. The CSAC is intended to be a temporary advisory body. Members will be appointed by the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, for an initial term commencing on the date of appointment and concluding no later than 15 June 2022.

16. The CSAC will have 8 members, including a Chair. The Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, will determine the membership of the CSAC.
17. The Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, has discretion to add or remove members, including the Chair. CSAC members may resign by informing the Minister for the Digital Economy and Communications and the Chair in writing.
18. The Terms of Reference may be reviewed periodically by the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, the Chair, and the CSAC members.

### **Criteria and expertise**

---

19. The CSAC will comprise private sector representatives, and may also include academia or civil society representation if so decided by Ministers.
20. The following criteria will be used to determine the CSAC membership:
  - i. *Domain knowledge*: Members need to bring relevant knowledge and experience in one or more of the following areas: cyber security, cloud, technologies, private sector governance, skills uplift, innovation, critical infrastructure security and resilience, supply chain security.
  - ii. *Awareness of the New Zealand context*: Members need to bring an understanding of the current cyber security landscape in New Zealand, including threats and issues being faced by organisations, as well as current cyber security capabilities and services in New Zealand.
  - iii. *Ability to think broadly and strategically*: Members need to be able to think strategically and creatively about the shifts required in the cyber security landscape to effect meaningful change on the overall direction of New Zealand's cyber security policy and strategy.
  - iv. *Commitment to improved cyber security in New Zealand*: Members must be able to see beyond their own interest areas, and bring a sector-wide view that will benefit the nation, rather than a narrow interest group or their own business.
  - v. *Collaboration*: It is critical that Advisory Committee members can work together to deliver advice, insights, and recommendations to government. The members would have demonstrated a strong ability to work with other individuals and groups, and consider perspectives different to their own.
21. In addition, members will represent a diversity of backgrounds (including in age, gender, and ethnicity) and expertise.
22. The CSAC may also draw on the knowledge of other experts that will not be members but may provide specific, expert advice. This may also include

individuals or counterpart councils overseas, who could bring insights and ideas to adopt or adapt in a New Zealand context.

### **Independence of advice**

---

23. Members (including the Chair) serve in a personal capacity unless otherwise indicated.
24. Members are appointed to provide expert impartial advice based on their knowledge and expertise. They are not appointed to represent the interests of any single sector, stakeholder or special interest group, unless explicitly provided for when appointed.

### **Conflicts of interest**

---

25. In making themselves available for appointment, members must declare and disclose that there is no actual, potential or perceived conflict of interest, that cannot be appropriately managed, which would preclude their appointment.
26. This will include:
  - Completing a formal Conflict of Interest Declaration; and
  - Notifying the CSAC Chair and Secretariat immediately should any additional conflict of interest arise during the time the CSAC is operational.
27. Where a conflict arises, it is up to the CSAC Chair to determine the appropriate action for mitigating the conflict, including excusing members from the relevant discussion, advice, or activity.
28. The Secretariat will maintain a register of such conflict declarations.
29. CSAC members accept that failure to declare a conflict of interest may result in their immediate removal from the CSAC.

### **Meetings**

---

30. Meetings of the CSAC will be held virtually, unless otherwise advised.
31. Meetings between the CSAC and responsible Ministers will be advised by the office of the Minister for the Digital Economy and Communications. Agendas will be provided in advance by the Minister's office.
32. Meetings between the CSAC and stakeholder government agencies will be advised and supported by the Secretariat. Agendas and papers will be provided in advance by the Secretariat.
33. CSAC members are expected to attend meetings wherever reasonably possible.

### **Secretariat**

---

34. The Department of the Prime Minister and Cabinet will host a Secretariat function for the CSAC, and will ensure there is appropriate support for the CSAC.

## **Media**

---

35. The CSAC, and CSAC members acting in that capacity, will not make media statements without the prior agreement of the Minister for the Digital Economy and Communications.
36. If the CSAC is asked to provide comment on any issue relating to cyber security by a third party (i.e. other than relevant Ministers or government agencies), the CSAC will forward the question or request to the Secretariat.
37. This section in no way limits any CSAC member making public comment in their individual or organisational role, only as a representative of the CSAC.

## **Remuneration and expenses**

---

38. CSAC members will be eligible for reimbursement in accordance with the Cabinet Fees Framework (Group 4, Level 2). The Chair will be paid a daily rate of \$885. Members will be paid a daily rate of \$560.
39. Reimbursement for expenses (e.g. travel and accommodation, if required) will be provided. Work other than preparation for meetings must be approved and minuted by the CSAC/Secretariat before it is undertaken.
40. The CSAC and its members will not have an independent budget.

## **Transparency and accountability**

---

41. CSAC members should assume that all information presented to them, whether written or in oral form, is public information and the principle of availability applies. The CSAC is subject to the OIA and the Public Records Act 2005 (along with other legislation), including all material produced for or by the CSAC.
42. All requests for the release of information under OIA will be handled by the Secretariat in consultation with the Chair and the Ministers' Offices.
43. The CSAC is subject to the Protective Security Requirements.
44. Members of the CSAC are not liable for any act or omission done or omitted in their capacity as a member, if they acted in good faith and with reasonable care in pursuance of the functions of the CSAC.

## **Confidentiality**

---

45. The work of the CSAC is confidential, unless otherwise agreed by the Minister for the Digital Economy and Communications.
46. The Committee may require information from other agencies and stakeholders. The Committee will engage with the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB, regarding information requirements and, at the direction of either Minister, the appropriate Office will liaise with the relevant agencies and officials to request such information.



47. Whilst operating openly and transparently, the CSAC will ensure that information confidential to the Committee (including but not limited to Intellectual Property (below), confidential information, work product, strategies or tactics, or any other matter that a reasonable person would consider private) is kept confidential to members of the CSAC, and will not disclose information about the operations of the CSAC to any person without the above agreement.
48. Members of the Committee must maintain confidentiality of matters discussed at meetings, and any information or documents (not otherwise publicly available) provided to the Committee.

### **Intellectual property**

---

49. All physical and intellectual outputs of the CSAC shall be the property of the Crown. For the avoidance of doubt this includes all reports, papers, electronic documents, software and recordings.
50. An exception to this may apply where outputs incorporate third party sources or IP from panel members. Such situations will be considered on a case-by-case basis.

### **Disestablishment of the CSAC**

---

51. The CSAC will be disestablished as of 15 June 2022, or may be disestablished at any other time by the Minister for the Digital Economy and Communications, in consultation with the Minister Responsible for the GCSB.

# CODE OF CONDUCT FOR CSAC MEMBERS

## **Purpose**

---

The Code of Conduct sets out expectations for the general conduct of Cyber Security Advisory Committee (CSAC) members. Members are advised that failure to comply with the Code of Conduct could result in the Minister considering their removal from the CSAC.

## **General expectations**

---

It is expected all Committee members, including the Chair, will:

- work in an inclusive, constructive and collaborative manner;
- raise the views of industry stakeholders and consider a wide range of perspectives from the sector, rather than a narrow interest;
- take collective responsibility for the actions and decisions of the CSAC;
- act in accordance with process and protocols agreed or mandated by relevant Ministers and the Chair;
- attend all scheduled meetings and undertake any required pre-meeting reading to ensure they can engage fully at each meeting;
- work transparently and consistent with all privacy, security and legal requirements, including but not limited to the requirements of the Official Information Act 1982 and the Privacy Act 2020;
- maintain and safeguard the confidentiality of information submitted to them or obtained in carrying out their role;
- disclose any real, potential or perceived conflicts of interest as they arise and agree to the appropriate management of these conflicts, in the manner determined by the Chair; and
- only claim for legitimate expenses they may incur.

## **Responses to media queries**

---

Where a journalist or media outlet seeks the views of an individual member, or another group the member may belong to or represent, the member will make clear that any views presented by them represent their personal views, or those of the other group they may represent, and not those of the CSAC.

## **Personal views**

---

Members are free to express a personal view in public or in the media at any time. When doing so they must observe the following:

- comments must make clear that they represent a personal view and must not state or imply that they represent the views of the CSAC;
- where a member may make a statement that is contrary to the agreed position of the CSAC, the member must not state or imply that their statements represent a majority view; and;

- comments to the media must observe the other general expectations of conduct, e.g., maintaining and safeguarding the confidentiality of information presented to them as a CSAC member.

## INFORMATION REGARDING PAYMENTS OF FEES TO CSAC MEMBERS

1. All members should complete the attached IR330C - Withholding Tax Declaration Certificate and return this to § 9(2)(k) . If you hold a Withholding Tax Exemption Certificate from IRD, please also provide this to § 9(2)(k) . Payment will not be possible until the relevant documentation is received.
2. Please see attached a sample format for invoicing. Members should number their invoice and include an email address for the remittance advice. Invoices should be submitted on a monthly basis.
3. The invoice should quote your GST number if you are registered for GST, and add the GST to the total invoiced. No GST will be added if you are not registered.
4. The amounts for fees should be subtotaled. Any expenses (if relevant) should be shown and totalled separately. Any claims for reimbursement of expenses will need to be accompanied by tax receipts.
5. Completed invoices should be sent to § 9(2)(k) . **Please submit these in Word document format.**
6. Once the invoice is submitted, DPMC Finance will deduct tax where applicable, and make payment to the bank account supplied on the invoice. The bank account where payment is to be deposited should be shown on the invoice.
7. Please note that there may be some delay in receiving the first payment while the appropriate systems are put in place – your patience at this time will be appreciated. Any questions, please contact § 9(2)(k)
8. If the member requires assistance with preparation of individual tax returns or requires further personal tax advice, they should refer to a Chartered Accountant. For additional information on taxation of Schedular Payments, please refer to the IRD website: <https://www.ird.govt.nz/income-tax/withholding-taxes/schedular-payments>

# Acceptance of Appointment form

I \_\_\_\_\_ (full name)  
accept the Terms of my Appointment as Chair/Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

I have no known conflicts of interest

OR

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement

Signature \_\_\_\_\_

Date        /        /

## Code of Conduct Agreement

I \_\_\_\_\_ (full name)  
understand and am willing to comply with the Code of Conduct for the Cyber Security Advisory  
Committee (CSAC).

**Signature** \_\_\_\_\_

**Date**        /        /

**INVOICE TO:**

Department of the Prime Minister and Cabinet  
Executive Wing  
The Beehive  
Wellington

**FROM:**

[insert full name, physical address and email address]

Date of Invoice:  
Invoice Number :

Cost centre reference: **094-302**

---

Panel Member Fees

Meeting [insert date of meeting]	\$
Reading time [if applicable]	\$
<hr/>	
Sub Total for Meeting Fees	\$
Meeting expenses (if applicable)	\$
GST (@15%) if applicable	\$ -
	<hr/>
TOTAL	\$ =====

Bank Account details: [insert bank account number]

Use this form if you're a contractor receiving schedular payments.

If you're receiving salary or wages as an employee, you'll need to use the *Tax code declaration (IR330)* form.

If you receive schedular payments you will receive an invoice for your ACC levies directly from ACC.

### Once completed:

**Contractor** Give this form to the person paying you.

**Payer** Don't send this form to Inland Revenue. You must keep this completed IR330C with your business records for seven years following the last schedular payment you make to the person or entity.

## 1. Your details

Full Name

IRD number (8 digit numbers start in the second box.

If you don't have:

- your IRD number you can find it in myIR or on letters or statements from us.
- an IRD number go to [www.ird.govt.nz](http://www.ird.govt.nz) (search keywords: IRD number) to find out how to apply for one.

## 2. Your tax rate

You must complete a separate *Tax rate notification for contractors (IR330C)* for each source of contracting income.

Refer to the flowchart on page 2 and enter your tax rate to one decimal point here.    %

Refer to the table on page 3 and enter your schedular payment activity number here.

Your tax code will always be:

WT

## 3. Declaration

Name

Designation or title  
(if applicable)

For example, director, partner, executive office holder, manager, duly authorised person

Signature

2 | 0  
Day Month Year

Give this completed form to your payer. If you don't complete sections 1 and 3 your payer must deduct tax from your pay at the no-notification rate of 45%, except for non-resident contractor companies where it's 20%.

### Privacy

Meeting your tax obligations means giving us accurate information so we can assess your liabilities or your entitlements under the Acts we administer. We may charge penalties if you don't.

We may also exchange information about you with:

- some government agencies
- another country, if we have an information supply agreement with them
- Statistics New Zealand (for statistical purposes only).

If you ask to see the personal information we hold about you, we'll show you and correct any errors, unless we have a lawful reason not to. Contact us on 0800 377 774 for more information. For full details of our privacy policy go to [www.ird.govt.nz](http://www.ird.govt.nz) (search keyword: privacy).

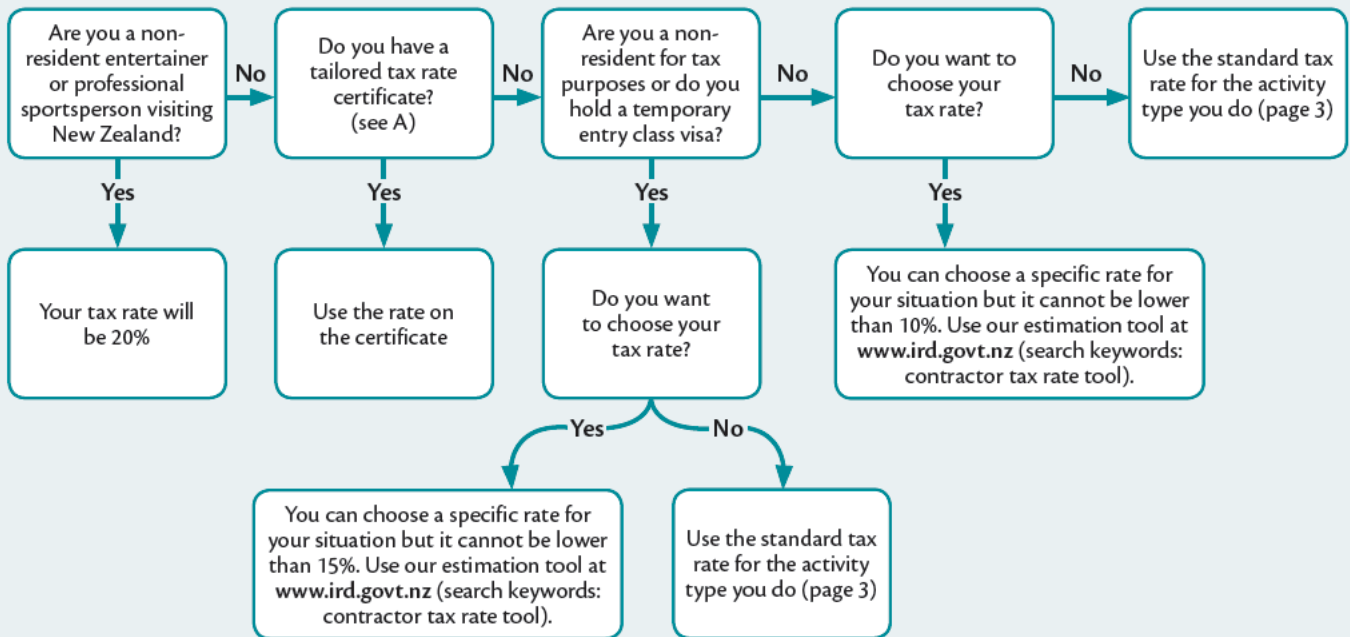
RESET FORM



Schedular payments are payments made to people who are not employees but are contractors. This includes independent contractors, labour-only contractors and self-employed contractors. You're receiving schedular payments if you're not an employee and the type of work you're receiving a payment for is an activity listed on page 3.

If you aren't ordinarily required to have tax deducted from payments you receive you can choose to have tax deducted. This will be treated as schedular payments, if the person paying you agrees. You will need to get their agreement in writing.

**Use the flow chart below to work out what tax rate to use**



A If you have a tailored tax rate (TTR) enter this on page 1 and show your original TTR certificate to your payer.

A TTR is a tax rate worked out to suit your individual circumstances. You may want a TTR if the minimum tax rate that applies to you will result in you paying too much tax. For example, if you have business expenses that will lower the amount of tax you need to pay on your income. You can apply for a tailored tax rate in myIR or by completing a *Tailored tax code application (IR23BS)* form. Go to [www.ird.govt.nz](http://www.ird.govt.nz) (search keyword: IR23BS).

If you're a non-resident contractor the application process is different. For more information go to [www.ird.govt.nz](http://www.ird.govt.nz) (search keywords: NRCT special rate).

B If you don't want tax deducted from your schedular payments, you may be able to apply for a certificate of exemption (COE) in myIR or by completing the *Request for PAYE exemption on schedular payments (IR332)* form on our website.

If you're a resident contractor paid by a labour hire business under a labour hire arrangement you cannot use a COE for these payments. You may be able to apply for a 0% tailored tax rate instead. You can complete an IR23BS in myIR.

For more information about COEs go to [www.ird.govt.nz](http://www.ird.govt.nz) (search keywords: schedular coe).

**Non-residents**

You can apply for a non-resident contractor certificate of exemption in myIR using the tailored tax code application. Send a secure mail with your enquiries about non-resident contractors in myIR or contact us:

Phone: 64 4 890 3056

Fax: 64 4 890 4502

Additionally, the following may be entitled to an exemption from tax:

- non-resident entertainers taking part in a cultural programme sponsored by a government or promoted by an overseas non-profit cultural organisation
- non-resident sports people officially representing an overseas national sports body.

Send a secure mail with your enquiries in myIR or contact us:

Phone: 64 9 984 4329

Fax: 64 9 984 3081

## Schedular payment tax rates

If you are receiving payment for any of the types of work listed below, enter the activity number in the box at section 2 on page 1.

The description below may not include all activities. For a more detailed description see schedule 4 of the Income Tax Act 2007.

You'll generally be required to complete an income tax return at the end of the tax year.

Activity number	Activity description	Standard tax rate – %	No-notification rate – %
1	ACC personal service rehabilitation payments (attendant care, home help, childcare, attendant care services related to training for independence and attendant care services related to transport for independence) paid under the Injury Prevention and Rehabilitation Compensation Act 2001	10.5	45
2	Agricultural contracts for maintenance, development, or other work on farming or agricultural land (not to be used where CAE code applies)	15	45
3	Agricultural, horticultural or viticultural contracts by any type of contractor (individual, partnership, trust or company) for work or services rendered under contract or arrangement for the supply of labour, or substantially for the supply of labour on land in connection with fruit crops, orchards, vegetables or vineyards	15	45
4	Apprentice jockeys or drivers	15	45
5	Cleaning office, business, institution, or other premises (except residential) or cleaning or laundering plant, vehicle, furniture etc	20	45
6	Commissions to insurance agents and sub-agents and salespeople	20	45
7	Company directors' (fees)	33	45
8	Contracts wholly or substantially for labour only in the building industry	20	45
9	Demonstrating goods or appliances	25	45
10	Entertainers (New Zealand resident only) such as lecturers, presenters, participants in sporting events, and radio, television, stage and film performers	20	45
11	Examiners (fees payable)	33	45
12	Fishing boat work for profit-share (supply of labour only)	20	45
13	Forestry or bush work of all kinds, or flax planting or cutting	15	45
14	Freelance contributions to newspapers, journals (eg, articles, photographs, cartoons) or for radio, television or stage productions	25	45
15	Gardening, grass or hedge cutting, or weed or vermin destruction (for an office, business or institution)	20	45
16	Honoraria	33	45
17	Modelling	20	45
18	Non-resident entertainers and professional sportspeople visiting New Zealand	20	N/A
19	Payment by a labour hire business to any person (eg individual, partnership, trust or company) performing work or services directly for a client of the labour hire business or a client of another person, under a labour hire arrangement	20	45
20	Payments for: <ul style="list-style-type: none"> <li>– caretaking or acting as a guard</li> <li>– mail contracting</li> <li>– milk delivery</li> <li>– refuse removal, street or road cleaning</li> <li>– transport of school children</li> </ul>	15	45
21	Proceeds from sales of: <ul style="list-style-type: none"> <li>– eels (not retail sales)</li> <li>– greenstone (not retail sales)</li> <li>– sphagnum moss (not retail sales)</li> <li>– whitebait (not retail sales)</li> <li>– wild deer, pigs or goats or parts of these animals</li> </ul>	25	45
22	Public office holders (fees)	33	45
23	Shearing or droving (not to be used where CAE code applies)	15	45
24	Television, video or film: on-set and off-set production processes (New Zealand residents only)	20	45
25	Voluntary schedular payments	20	45
	If you are a non-resident contractor receiving a contract payment for a contract activity or service and none of the above activities are applicable, then:		
26	Non-resident contractor (and not a company)	15	45
27	Non-resident contractor (and a company)	15	20

Note: If you need help choosing your tax rate use the estimation tool at [www.ird.govt.nz](http://www.ird.govt.nz) (search keywords: contractor tax rate tool)

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Hamish,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,



Hon Dr David Clark

Minister for the Digital Economy and Communications

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Jon,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,



Hon Dr David Clark

Minister for the Digital Economy and Communications

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Mike,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,

A handwritten signature in blue ink, appearing to be 'David Clark', written in a cursive style.

Hon Dr David Clark

Minister for the Digital Economy and Communications



# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Sheridan,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,

A handwritten signature in blue ink, appearing to be 'David Clark', written in a cursive style.

Hon Dr David Clark

Minister for the Digital Economy and Communications

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Steve,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)  
[Redacted text block]

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,



Hon Dr David Clark

Minister for the Digital Economy and Communications

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Vanessa,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## A single front door for reporting cyber incidents

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,



Hon Dr David Clark

Minister for the Digital Economy and Communications

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



3 June 2022

Dear Victoria,

In December 2021, I and Hon Andrew Little convened the Cyber Security Advisory Committee (CSAC) for a six-month period to provide independent, industry-centric advice to government on options for lifting New Zealand's cyber security and resilience. As this initial term draws to a close, I wish to thank you for the dedication and enthusiasm you have applied to this task. The quality of the CSAC's outputs and the calibre of the advice delivered across the four workstreams outlined in your Terms of Reference are commendable.

As you will be aware, the CSAC's advice has supported the work shortly being presented to Cabinet on lifting cyber security and resilience in the wider economy. The recommendations in the advice you delivered in March, alongside the findings of interagency workstreams, have been instrumental in determining three priority initiatives we will be proposing to Cabinet, namely:

- developing a compliance regime for minimum mandatory cyber security standards for Nationally Significant Organisations (NSOs) and critical infrastructure;
- introducing mandatory cyber incident reporting requirements of significant cyber incidents and ransom payments for NSOs and critical infrastructure and sectors; and
- the creation of a 'single front door' for the public to report cyber incidents.

While the report back to Cabinet will focus on progressing the priority initiatives above, I thank you for the breadth of recommendations you made in your report. There is a high degree of convergence between the additional recommendations you made and a number of ongoing workstreams by government, including as part of the implementation of the 2019 Cyber Security Strategy. I would be pleased to direct officials to brief you on this at your convenience.

s 9(2)(f)(iv)

Subject to approval by Cabinet, I intend to extend the CSAC's term for a further four months, and thank you for your willingness to continue your appointment. I am writing to provide you with further detail on my intentions for your work programme for this extended term.

## **A single front door for reporting cyber incidents**

In line with your recommendation, subject to approval by Cabinet, Hon Little and I intend to task officials with developing a programme of work to deliver a single front door for providing companies, organisations, and individuals a place for reporting cyber incidents, obtaining incident management advice, and where appropriate, practical help to respond and recover.

Industry-centric perspectives would be of great value as this work progresses, and I ask that you make this a central workstream during your extended term.

It is important to clarify that I do not currently consider that a new agency or entity is required, nor that current organisations need to be merged to deliver an effective single front door. I also do not envisage that the single front door itself would have additional functions such as providing proactive communications on cyber security: those functions would remain the responsibility of current lead agencies. Within that context, I would appreciate specific advice on the following aspects of design and implementation:

- key components and considerations to bear in mind for the design of a victim-centric 'single front door';
- partners with whom to engage on building a Te Ao Māori focus, and giving effect to Te Tiriti in the design of a 'single front door'; and
- how to maximise the benefits to the business sector arising from improved data collection on cyber threats and trends at central government level.

I believe there would be value in a joint discussion with officials as you commence your term extension to discuss these considerations in more detail, as well as to receive briefing on the work in this area to date and necessary background material. I would be pleased to direct officials to engage with you directly on this point, and would encourage you to meet regularly with officials as this work progresses for the duration of your term extension.

Beyond this, I would also appreciate the CSAC making itself available to provide views on the finalised Cabinet paper on cyber security in the broader economy – which has been shared with you in draft form – following its presentation to Cabinet in early June. Assuming it is approved by Cabinet through that process, I would welcome the CSAC's views in particular on industry priorities under the key initiatives proposed, and key considerations for a work programme to implement them.

Finally, I would welcome the CSAC's making itself available to review work arising from Cabinet decisions in December 2021 on lifting New Zealand's cyber security and resilience in the public service, if requested.

I look forward to receiving your advice on these matters, and take this opportunity to thank you once more for your contribution to this Committee.

Yours sincerely,

A handwritten signature in blue ink, appearing to be 'David Clark', written in a cursive style.

Hon Dr David Clark

Minister for the Digital Economy and Communications



# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Hamish,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[REDACTED]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark

**Minister for the Digital Economy and Communications**

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Jon,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[Redacted]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark  
**Minister for the Digital Economy and Communications**

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Mike,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as Chair of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[REDACTED]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your leadership of the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark

**Minister for the Digital Economy and Communications**

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Sheridan,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[Redacted]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark

**Minister for the Digital Economy and Communications**



# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Steve,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[Redacted]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark

**Minister for the Digital Economy and Communications**

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Vanessa,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[Redacted]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark  
**Minister for the Digital Economy and Communications**

# Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs  
Minister for the Digital Economy and Communications  
Minister for State Owned Enterprises  
Minister of Statistics  
Minister Responsible for the Earthquake Commission



23 November 2022

Dear Victoria,

With the Cyber Security Advisory Committee (CSAC)'s term now at a close, I wish to thank you for the contribution you have made as a member of this Committee.

Hon Andrew Little and I convened the CSAC in December 2021 to provide industry-centric perspectives on opportunities to lift New Zealand's cyber security and resilience. I thank you and your CSAC colleagues for the high calibre advice you provided, across a broad range of workstreams, and the Committee's spirit of collaboration with officials and Ministers.

Over the past ten months, the CSAC has provided considered advice on a range of policy questions. You began your term with work to deliver insights on cyber security policy, and the design of cyber security services to support business, as well as opportunities to bring together the collective expertise of the cyber security ecosystem. As outlined to you in my correspondence of 3 June, the CSAC's advice was instrumental in identifying the initiatives approved by Cabinet in June to lift cyber security across the economy. The CSAC's advice, received 28 June, did an excellent job of contextualising and sharpening the advice you provided previously. I commend the ambitious vision and broad thinking you applied to this paper, as well as the outreach you undertook to ground your thinking in the lived experience of businesses.

I also appreciated the perspectives you shared on the paper Hon Little and I presented to Cabinet in June - 'Cyber Security – Strengthening resilience in the wider economy'. As noted, the three core initiatives outlined in the Cabinet paper were informed by your hard work - I recognise your focus on the need to effect rapid change through expeditious implementation of these workstreams.

## *Single front door*

The CSAC's term extension has enabled you to develop focused advice on key considerations for the design and establishment of a single front door. Hon Little and I appreciate the work you have put into your final advice, and your vision for a single front door. Hon Little and I,

along with other Ministerial colleagues with relevant portfolios, are now considering how best to effect change to cyber incident reporting, for which your advice is a valuable input.

*Critical infrastructure*

As you are aware, the June Cabinet paper also recommended the development of a compliance regime for minimum mandatory cyber security standards, and mandatory cyber incident reporting requirements for Nationally Significant Organisations and critical infrastructure. In this, the CSAC's input has been invaluable. Work in these two areas - including consideration of a positive obligation on critical infrastructure operators to meet standards for cyber security - is set to progress at pace, as Ministers recognise the importance of enhancing the resilience of our critical infrastructure. Your insights on these topics in your report backs have been valuable inputs to the ongoing development of this work.

s 9(2)(f)(iv)

[Redacted]

While the CSAC and its funding arrangements formally ceased on 15 October, I hope to remain connected on an informal basis if your schedule permits. As respected industry representatives, you bring unique experiences to inform our thinking and I hope to continue to benefit from your valuable perspectives as relevant occasions arise.

Thank you once more for your contribution to the CSAC, and for the enthusiasm and dedication you have brought to this work.

Yours sincerely



Hon Dr David Clark

**Minister for the Digital Economy and Communications**

# ENCLOSURE 3: CONFLICT OF INTEREST FORMS


## Acceptance of Appointment form

I **Michael Charles John O'Donnell** accept the Terms of my Appointment as **Chair** of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

**I have no known conflicts of interest**

s 9(2)(a)



Signature \_\_\_\_\_

Date           **16/12/21**

## Acceptance of Appointment form

I Hamish John Rumbold (full name)  
accept the Terms of my Appointment as Chair/Member (delete as appropriate) of the Cyber  
Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

I have no known conflicts of interest

~~OR~~

~~That all other known conflicts of interest are listed below together with the  
arrangements which have been put in place to manage these.~~

Known conflicts of interest	Management arrangement

Signature

s 9(2)(a)

Please note I am currently CDTO of  
Kiwibank which I do not believe creates  
a conflict of interest.

Date

20, 12, 21



# Acceptance of Appointment form

**Jonathan Duffy**

I \_\_\_\_\_ (full name)  
accept the Terms of my Appointment as Chair/Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

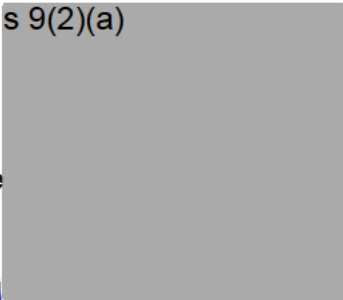
I declare that (circle the option which applies)

I have no known conflicts of interest

OR

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement
Former Board member - Netsafe	No longer Board member.

Signature  \_\_\_\_\_

Date 16/12/2021

# Acceptance of Appointment form

I Amanda Rhean Simpson (full name) accept the Terms of my Appointment as Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

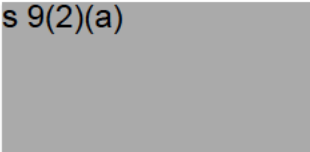
I declare that (circle the option which applies)

I have no known conflicts of interest

OR

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement

s 9(2)(a)  


Signature \_\_\_\_\_

Date 17 /12 /21

## Acceptance of Appointment form

I, SHERIDAN ADELENE BROADBENT accept the Terms of my Appointment as Member of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement
<p>Chair, Kordia Group (Aura Information Security and SecOps)</p> <ul style="list-style-type: none"><li>- As Chair of an organisation that is a provider of cyber security services in a competitive market there may be rare occasions where discussion or decisions may relate to services that Kordia may be providing or pitching for. This is an unlikely conflict and one that should be easy to manage while on CSAC.</li></ul>	<ul style="list-style-type: none"><li>- Abstain from any votes or decisions where Kordia Group may be, or may be perceived to be the beneficiary or related party</li><li>- Highlight any potential areas of conflict with the board chair prior to any meetings</li><li>- Secretariat to redact any information from papers which may cause conflict between my CSAC and Kordia roles</li><li>- Exit, at the request of the Chair, any discussions or meetings at which a matter in conflict with my role with CSAC arises,</li></ul>

s 9(2)(a)

Signature \_\_\_\_\_

Date

16/12/2021

## Acceptance of Appointment form

I Stephen James Honiss, (full name) accept the Terms of my Appointment as ~~Chair~~/Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

~~I have no known conflicts of interest~~

OR

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement
Financial interest in, and employee of, ZX Security Ltd (Director of Cyber Strategy & Risk)	<ul style="list-style-type: none"> <li>• Advise Chair (already aware) and other committee members at first meeting</li> <li>• Restate role and interests where a real or perceived conflict arises and where deemed necessary, recuse myself from aspects of the work</li> <li>• Ensure that advice to Ministers is delivered jointly rather than by myself</li> <li>• Note that ZX Security has a strong Environmental, Social and Governance ethos and our interest is in better security outcomes for NZ with our business interests being secondary</li> </ul>
Director of Netsafe	<ul style="list-style-type: none"> <li>• Advise Chair (already aware) and other committee members at first meeting</li> <li>• Restate role and interests where a real or perceived conflict arises and where deemed necessary, recuse myself from aspects of the work</li> <li>• Ensure that advice to Ministers is delivered jointly rather than by myself</li> <li>• Note I have no financial interests in Netsafe as a charity and there is unlikely to be any material conflict arising</li> <li>• Disclosing in the interests of transparency</li> </ul>

Signature \_\_\_\_\_

**Date**       /     /

# Acceptance of Appointment form

I, Vanessa Ngaroimata CLARK (full name) accept the Terms of my Appointment as Chair/Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

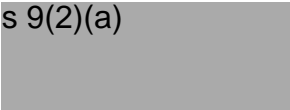
I declare that (circle the option which applies)

**I have no known conflicts of interest**

OR

~~That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.~~

Known conflicts of interest	Management arrangement

Signature \_\_\_\_\_  \_\_\_\_\_

Date **17 / 12 / 2021**

## Acceptance of Appointment form

**Victoria Pauline MacLennan**

I \_\_\_\_\_ (full name)  
accept the Terms of my Appointment as Chair/Member (delete as appropriate) of the Cyber Security Advisory Committee (CSAC) as outlined in the attached Appointments Letter.

I declare that (circle the option which applies)

~~I have no known conflicts of interest~~

OR

That all other known conflicts of interest are listed below together with the arrangements which have been put in place to manage these.

Known conflicts of interest	Management arrangement
Perceived conflicts <ul style="list-style-type: none"><li>• Government Relations role with NZRise</li><li>• Owner OptimalBI</li><li>• Noted Limited</li></ul>	No real conflict however declaring as could be perceived conflict of interest.  No management arrangement required.

Signature  s 9(2)(a)

Date 20 / December / 2021