DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Proactive Release

The following documents have been proactively released by the Department of the Prime Minister and Cabinet (DPMC), on behalf of Hon Ginny Andersen, Minister for the Digital Economy and Communications.

[Proactive Release] Cyber Security Advisory Committee (CSAC) documents

The following documents have been included in this release:

Title of paper: New Zealand Cabinet Cyber Security Advisory Committee Report back on Workstreams 1/2/3

Title of paper: Proposal on Cyber Security Single Front Door

Title of paper: Briefing: Reflections on CSAC Advice and Next Steps

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant section of the Act that would apply has been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to redaction codes:

- section 9(2)(ba)(i), to protect the supply of similar information in the future
- section 9(2)(g)(ii), to prevent improper pressure or harassment
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials
- section 18(d), that the information requested is or will soon be publicly available

This document is a report by the Cyber Security Advisory Committee (CSAC). The CSAC was an independent industry advisory committee, appointed by Ministers.

This document does not represent government advice or government policy.

NZ Cabinet Cyber Security Advisory Committee

Proposal on Cyber Security Single Front Door

Scope

What's in scope for the single front door?

- All trading entities and enterprises – from sole trader to NZ arm of multinational, Post Settlement Governance Entities, commercial/non profit/charitable, private/public.
- Cyber incidents, cybercrimes (e.g. system compromises, ransomware, data breach, unauthorised system access, etc).

What's out of scope for the single front door?

- By group – NSOs, non-business: individuals, mums and dads.
- By attack vector - HDC victims, image abuse, intimidation, romance scams, individual financial fraud and identity theft.

CSAC timeline

Dec 21 CSAC formed – 4 terms of reference

Feb 22 CSAC delivers findings on:

- Capability
- Cyber security framework
- Private collaboration forum

March 22 CSAC delivers customer orientation study findings

June 22 CSAC delivers Supplementary Issues paper

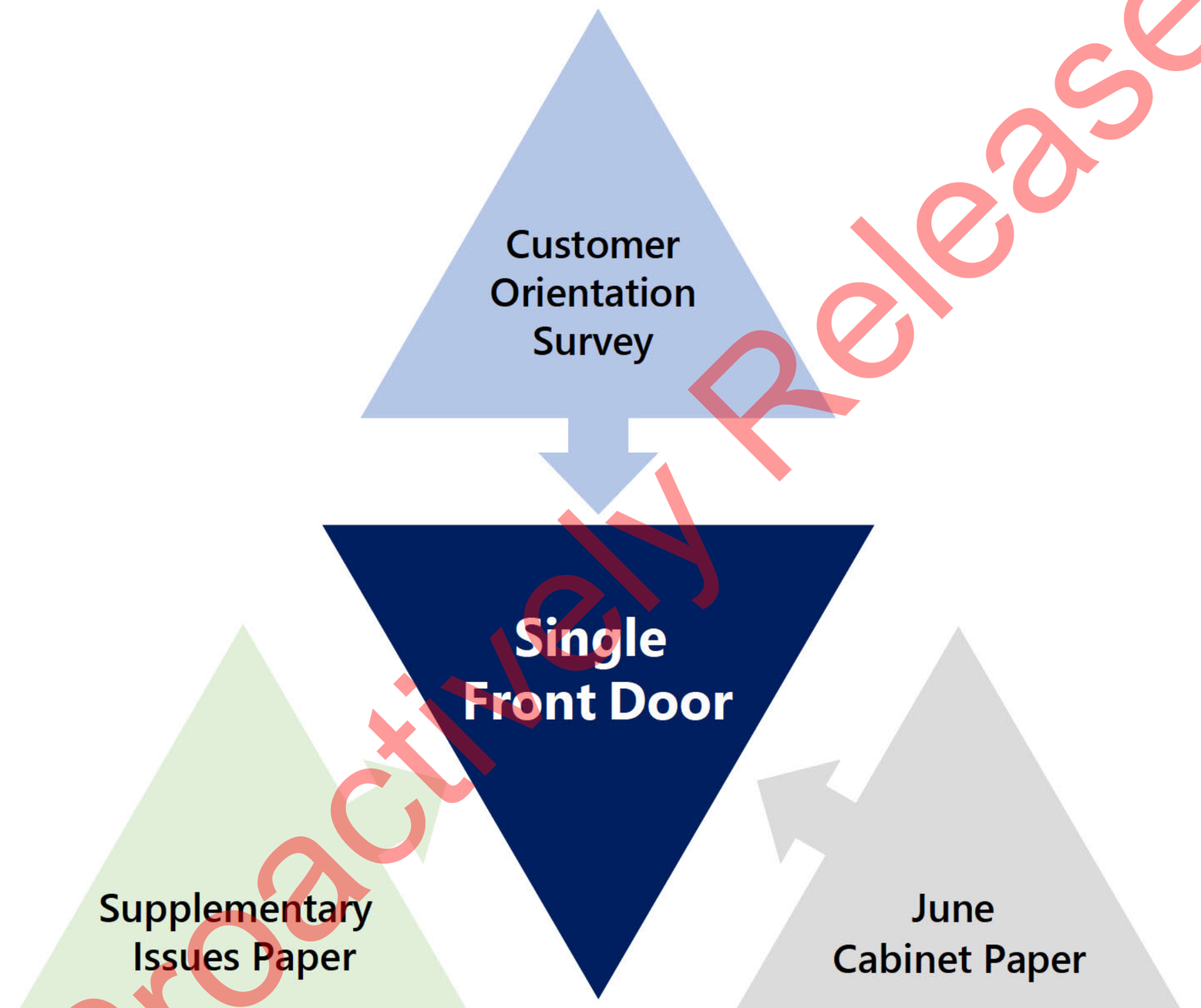
July 22 CSAC review of June Cabinet paper

Sept 22 SFD draft to agencies for feedback, gather other insights

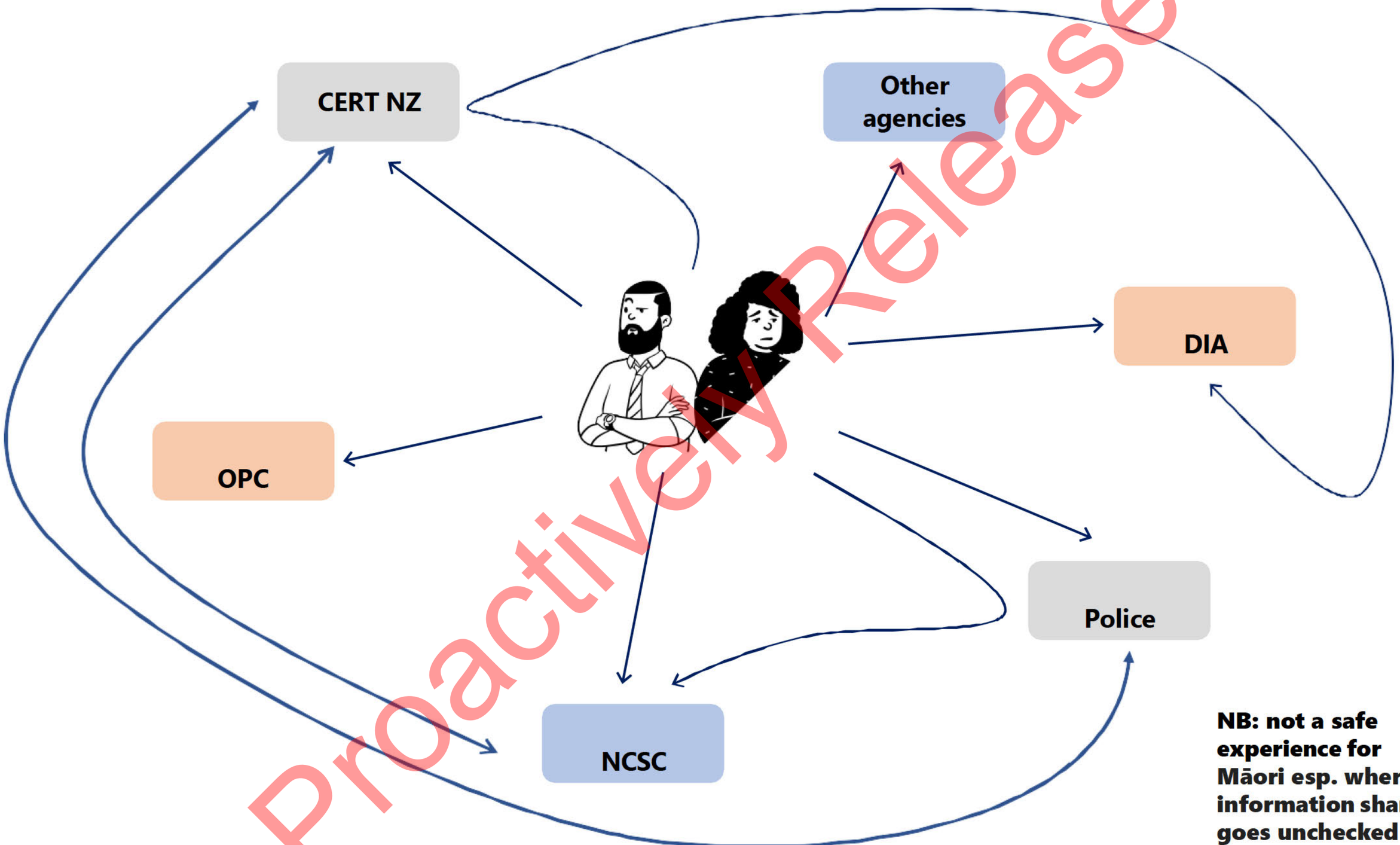
Sept 22 CSAC finalises SFD proposal

15 Oct 22 Final SFD recommendations to Ministers

The Single Front Door concept fell out of all workstreams



Current merry-go-round experience for business victims



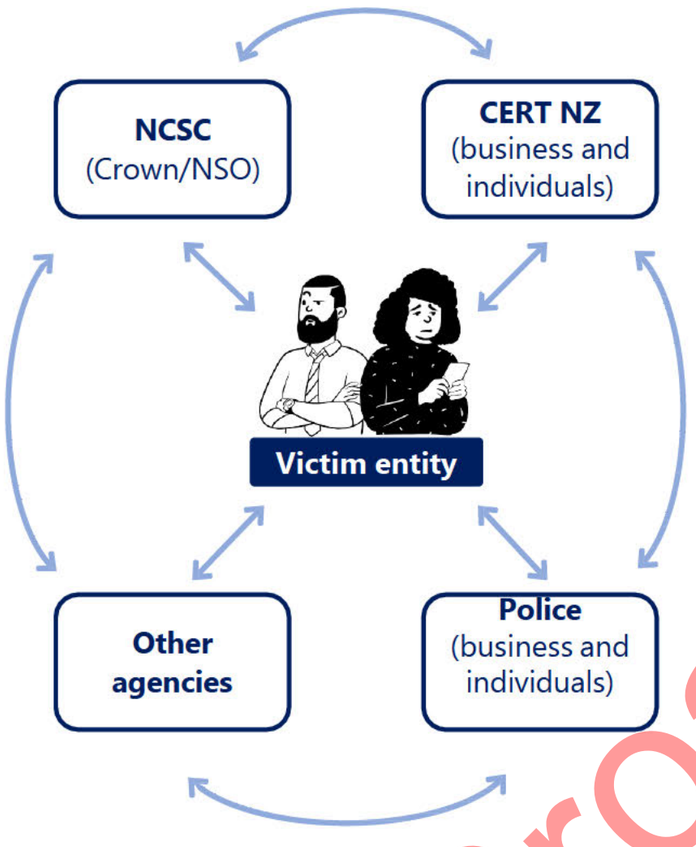
NB: not a safe experience for Māori esp. where information sharing goes unchecked

Proposed victim experience: Single Front Door

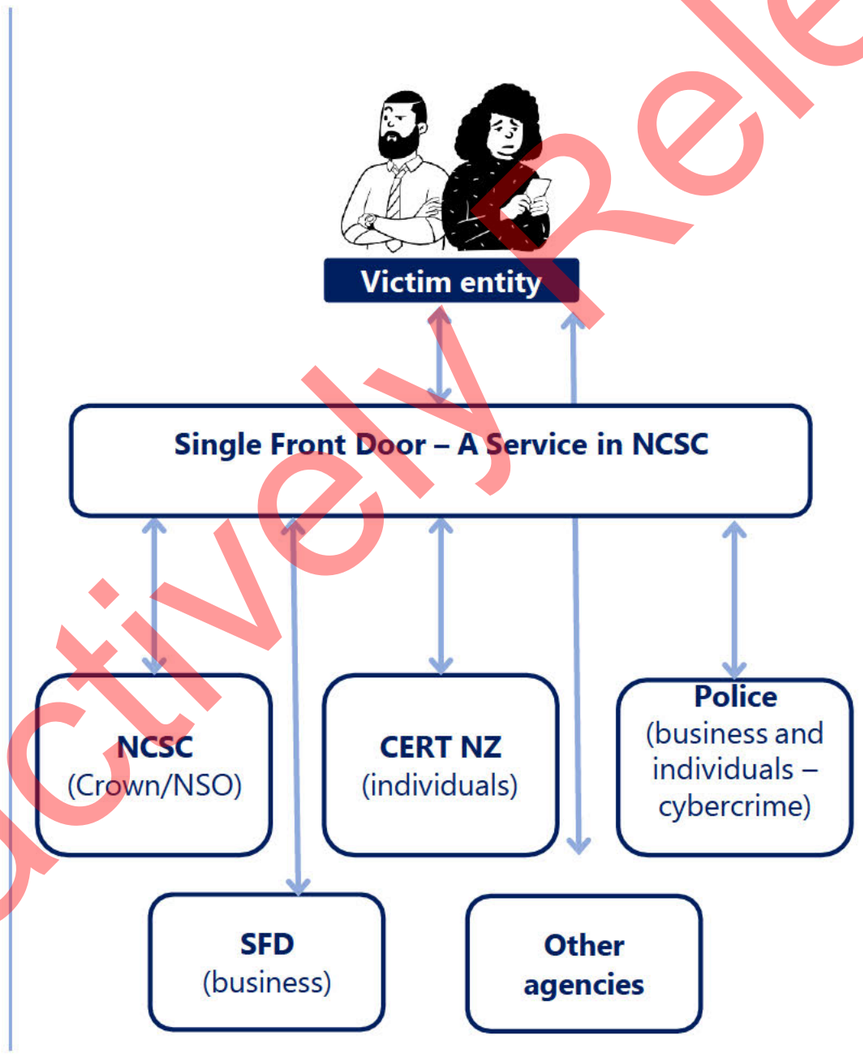
- An alternative to a single agency, when you don't have a single agency.
- The Single Front Door swings both ways …
    - Proactively keeps in touch with the victim AND works with them until affected systems are recovered.
    - Victim centric case management oversight until the case is closed.
- Single Front Door = No Wrong Door
    - If a business makes initial contact via other means (eg Police/NCSC/CERT and in some cases Netsafe), these agencies capture details and share them with SFD.
    - In most cases SFD becomes the victim's case overseer (except police investigations + NSOs) but victim can still deal directly (e.g. for OPC and FMA).
- SFD accountable for triage, shepherding and reporting; also provides incident reporting rates by sector and incident type, case closure rates and victim satisfaction stats to government.
- Provides a single, simple victim reporting portal (similar to ACSC's "Report Cyber") with relevant agency feeds.
- Also worth considering a cyber security minister for policy, strategy and cross government input (as per Australia).

Stepping stone to target future state

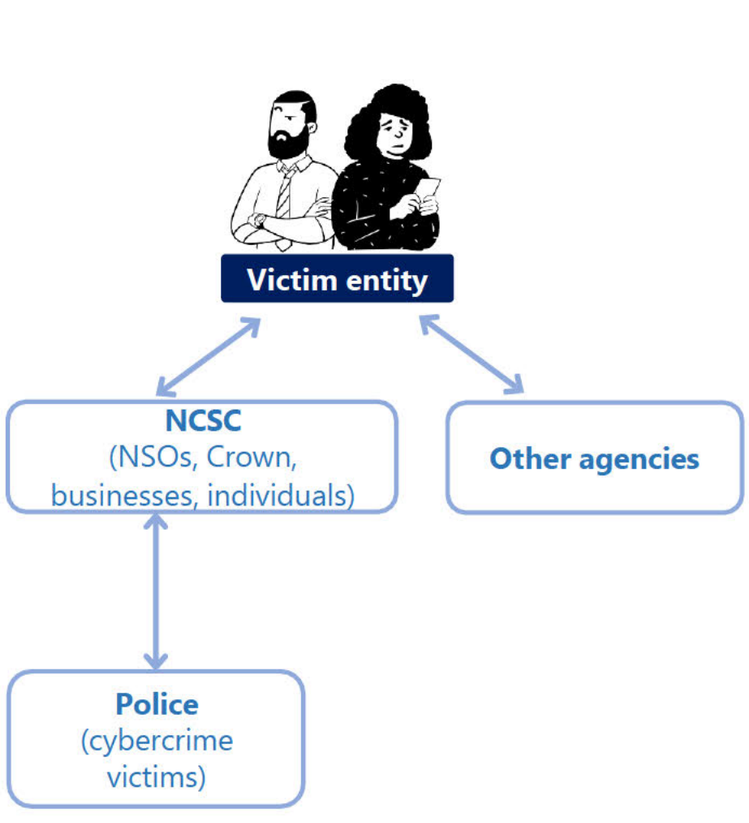
Current victim experience



SFD: interim victim experience



Future victim experience



NB – For SFD and target end state – Te Tiriti will be baked into the triaging and response.

Single Front Door: victim use case insights

CSAC developed five attack use cases (see **Appendix 1**).

These take a user-centric approach to the lifecycle of a cyber attack to capture key points of contact, assistance provided, handover points and expected outcomes.

Key insights were:

- Multiple handoffs are a risk; a single group accountable for oversight of all business cases would add significant value.
- Victims do not know what "box" they fit into and often situations escalate across sectors, software platforms and ecosystems; 'cradle to grave' stewardship will afford best opportunity to act early, warn others and build a shared knowledge base.
- Netsafe has a role to play in some cases, particularly where engagement with social media or hosting providers is required.
- Inter and intra-agency collaboration is paramount – events can require real time responses. Gravitas and mandate will be required to shepherd large and disparate interest groups and maintain oversight even when a significant event is being led by one agency.
- Cultural sensitivity is a must. Cyber security incidents involving Taonga, cultural identity or Te Tiriti implications require specialised triage and victim management. SFD triaging can take lessons from e.g. Whakarongorau NZ Telehealth Services who worked with iwi-affiliates and Māori partners, establishing specialised call centres during the pandemic.

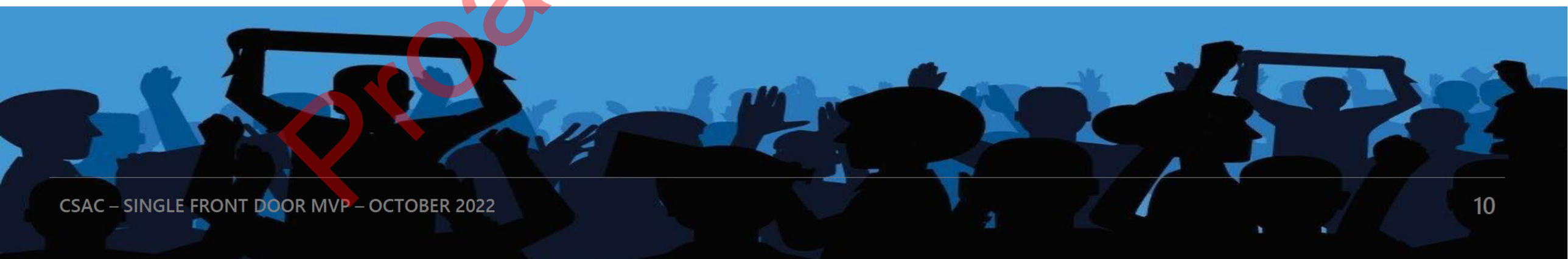
So why have the Single Front Door sitting in NCSC?

1. Consistent with Five Eyes nations; NCSC has deeper connectedness to what's happening in the global and local intelligence environment.
2. NCSC have useful empowering legislation.
3. CERT's position within MBIE creates possible focus and line-of-sight risks (CERT has been funding constrained).
4. NCSC have access to classified and unclassified intelligence, which along with the technical expertise of Five Eyes partners, can put the incident in context.
5. Many of the larger business cyber attacks are from state sponsored actors (or associated with them).
6. Many businesses in the CSAC survey reported NCSC as being useful and practical in supporting them to resolve their problem.

But …

If SFD is to be part of NCSC and sit alongside the existing engagement and outreach division then:

1. NCSC needs substantial new funding (people, platform, process, tools) in addition to any increase associated with merging agencies.
2. CERT is doing good work, has good tools and talent – this should be integrated into the SFD with change oversight driven by what's best for NZ.
3. SFD needs huge cultural orientation change – not trivial for NCSC.
4. NCSC needs to build authentic transparent relationships with iwi + Māori.
5. SFD leader will need proven private sector experience in delighting customers and user centricity.



Minimum viable product: SFD 1.0

What it is:

- A channel for all businesses in Aotearoa when they have experienced a cyber attack + need help to continue to trade.
- A trusted advisor who can help them understand what has happened and what the stages are to fixing it.
- A friendly voice/email to support them as they go about solving their own problems, and help shepherd them through the cyber security incident ecosystem.
- Someone who can save them time and money by providing victim centric information as and when needed.
- A one stop shop for businesses reporting a cyber security attack, the details of which will then be passed on relevant agencies as appropriate.
- A resource with proactive playbooks, training and informed resources. Small enough to be co-ordinated but smart enough to be making world class oversight, handover and response decisions. NB: if resources are in Māori then te reo triage should also be available.
- Harnessing a well-designed and resourced triage process. In particular, seamless referral to Police of relevant incidents is key.

What it isn't:

- An outsourced security service – no "blokes in vans with spanners".
- A substitute for specialist knowledge already within CERT, NCSC, Police, Netsafe or a security consultancy.
- A place to expect the government to fix things for free when businesses haven't taken appropriate security measures (cf: Police attending a burglary. They won't fix your windows or pay to get your door replaced).
- A greenfield project – there is already good work being done we can take forward.

Value add by victim type

For smaller businesses	It helps them understand the attack and provides them with the knowledge and connections to help them resolve it and get trading again.
For larger businesses	It helps them run their own process where the victim will corral a number of specialists (internal and external) who together will confirm the problem, provide advice on resolution, drive the implementation and help get the target business trading normally again. (War room sits at victim end).
For Māori enterprises	The ability to report a cyber security incident with cultural/Te Tiriti ramifications, such that it is fully responded to in an sensitive manner. *NB: Real chance to be a world leader on this as currently no-one does it well (that we have been able to find).*
For individuals	Individuals would have their details recorded and then be redirected to CERT NZ along with those details - i.e. SFD is not replacing CERT for citizens.
For NSOs	NSOs would have their case details recorded and then be redirected to incident response team in NCSC along with those details.
For Police matters	Victims would have their case details recorded and then the case details are redirected as a matter for NZ Police.

Value add by channel

Customers	Channel	**Total addressable market** (approximate)	**Estimated cyber security incidents handled** (per annum)
NSOs + key providers	NCSC	600	500
Businesses	SFD	557,680	680
Individuals	CERT NZ	4 million	7,500
Individuals + schools	Netsafe	4 million	10,000
Victims of cyber and cyber-enabled crime	NZ Police	5 million	Est. 25,000 +
	DIA	5 million	DIA received approximately 892,500 complaints in FY22 *

** n.b. of which 700,000 complaints were in relation to FluBot*

Where to from here?

- There is a significant gap between the current state and a high performance future state for cyber security prevention and defence. This document represents a call for action for investment in change.
- Government will now firm up organisation design, legislative requirements (if any), funding and resourcing of a minimum viable product of a SFD located inside NCSC.
- A key component will be the SFD reporting tool (which will feed to other agencies).
- CSAC members may be available to provide private sector oversight of the process if deemed useful.

Appendices

Appendix 1: Use cases for SFD

Appendix 2: DPMC study questions

Appendix 3: CERT NZ Original/Current Mandate

Appendix 4: Lessons and challenges shared by CERT NZ

Appendix 5: Possible touchpoints between OPC and SFD

Appendix 6: Current government investment

Appendix 1: Use case examples for Single Front Door

Incident happens	First contact /triage	The Fix	Follow-up	System-level activities
Account management				
Use case 1: Bob's Plumbing (small business) (hijacked credentials, ransom demand to allow banking, CRM and Xero access) **Victim feels:** • Annoyed • Confused • "Don't have time" • "Just want it sorted" **Victim needs:** • To pay bills and staff • To look clients up • To understand what's happening/what to do	**Use case 1: Bob's Plumbing** • Goes to Police first – transferred to SFD (omni-channel – all doors lead to the SFD). • SFD captures incident details once, shares them with Police, CERT + NCSC. • SFD responder providers initial diagnosis.	**Use case 1: Bob's Plumbing** • SFD helps "bucket up" the fix. • Provides playbook covering off: o Reset passwords, set up MFA o Advice on resetting access to SaaS CRM provider o Who to contact and how at victim's bank fraud team. • Bob is responsible to overseeing the fix, but SFD follows up over following days to help shepherd him.	**Use case 1: Bob's Plumbing** • Once resolved, provides email advice on avoiding a 'next time'. • Follow up call two weeks later to see how Bob is tracking and any outstanding issues.	• Works with professional bodies to prevent repeat incidents (e.g. Bankers' Association, NZITF, InternetNZ, NZTech, IT Professionals) • Maintains relationships with national Māori organisations • Analyses metadata from incidents • Embeds Te Tiriti in the triage process. • Broader data sovereignty and data governance considerations.
Use case 2: Aoraki College (medium) (phishing leads to false invoicing + payment) **Victim feels:** • Overwhelmed • Confused • Fish out of water • Concerned about reputation **Victim needs:** • To know what to do • Advice on what to tell the students • Diagnosis of the problem • To stop this from happening again	**Use case 2: Aoraki College** • Contacts via phone. • Capture initial incident details shares details with Police, NCSC and CERT. • SFD responder gives initial prognosis of what has happened.	**Use case 2: Aoraki College** • Refers victim to AoG panel of private security consultants to find a trusted partner to help manage the fix. • SFD provides: o Response checklist/playbook o Comms advice (scripts) for students and public o Connections to previous victims who have experienced the same thing and been through the fix process o Advice on who to contact for insurance and privacy elements (Police, OPC) o An outline of what each of the three core agencies does and works with those agencies on the victim's behalf.	**Use case 2: Aoraki College** • SFD provides follow up calls/emails to check on how fix is going. • SFD determines if its playbooks/checklists need updating in light of learnings from this incident.	
Use case 3: Acme Funds Management (large $10b) (DDoS site takedown with ransom demand) **Victim feels:** • Alarmed/concerned • Unsure what to expect • "Worst nightmare" • "Tempted to pay ransom to buy time to put in proper fix **Victim needs:** • Practical advice • Clarity – can SFD help, if not, who can? • Advanced tech support, gap analysis on response plan • To know if others are experiencing this	**Use case 3: Acme Financial Services** • Contacts via phone. • Capture initial incident details and shares details with Police, NCSC and CERT. • SFD sends confirmation email meeting reporting requirements for the victim to be able to commence cyber insurance claim. • SFD outlines what each of the core agencies does, what help they can provide the victim and acts as the victim's conduit to them.	**Use case 3: Acme Financial Services** • Ideally the victim will put into action an enterprise level cyber incident response plan (IRP) – a case manager will arrange appropriate agency to participate. • If victim does not have a security partner or IRP they are provided details of the AoG panel of private security consultants and playbook around IRP responses. • Connect to others who have experienced the same thing • Advice on who to contact: o OPC o FMA (or other statutory reporting requirements) o ISPs.	**Use case 3: Acme Financial Services** • Give victim transparency on progress of their case – proactive updates by phone. • Once resolved, advice on avoiding a 'next time'. • SFD determines if its playbooks/checklists need updating in light of learnings from this incident.	
Use case 4: Large iwi post-settlement governance entity (large $50b) (phishing leads to loss of tribal whakapapa repository) **Victim feels:** • Responsible • Overwhelmed • Worried • Whakamā **Victim needs:** • To prevent further loss • To secure compromised systems • To make decisions on the ransom • To keep communications limited • To navigate a relationship with Police	**Use case 4: Large iwi post-settlement** • SFD captures incident details once, shares them with Police and CERT. • SFD provides culturally appropriate support (e.g. trigger questions that sees the approach going through a separate triage pathway). • Provides advice on paying a ransom (pros and cons, reality check on likelihood that data will be returned). • Provides an outline of what each of the three core agencies does and works with those agencies on the victim's behalf.	**Use case 4: Large iwi post-settlement** • Victim given playbook on theft of sovereign data. • If victim does not have a security partner they are provided details of the AoG panel of private security consultants. • Advice on who to contact: o TPK o Police.	**Use case 4: Large iwi post-settlement** • SFD provides follow up calls/emails to check on how fix is going. • SFD determines if its playbooks need updating in light of learnings from this incident.	

Appendix 2: DPMC study questions

Q: What would businesses expect in terms of the level of service for incidents of various degrees of impact/severity?

A: We would expect a standard service of 7am-7pm, 5 days a week, with an afterhours service for more serious cyber security incidents.

Q: Would there be a categorisation/prioritisation of some kind?

A: Absolutely. We would need a point scoring system similar to that used by the ACSC that plots size of organisation along with intensity of attack (nature of org could also be a factor).

Q: What would businesses expect in terms of online interaction with the SFD?

A: They would expect to hear back from a SFD triage officer within an appropriately rapid response time – via email or on the phone.

Q: What role does the CSAC see for a SFD in supporting individual victims of cyber security incidents?

A: The SFD will not provide support for private individuals but would capture details and hand them across to CERT.

Q: What role does the CSAC see for a SFD around cybercrime victims?

Q: What role does the CSAC see for a SFD around cybercrime victims?

A: The SFD will take the details of the victim and the crime and pass them to Police (as CERT does also).

Q: What is a typical customer experience look like for a victim business contacting SFD? (Indicatively – we are at the start of the process).

A:
1. A bespoke response/phone or email within as little as 1 business hour according to the severity of the event.
2. An initial diagnosis of what has happened to the victim and an overview of what the fix might include.
3. Victim provided with a list of AoG approved private sector cyber security companies if needed.
4. Victim given a playbook (and other material) relevant to their situation.
5. Having the SFD outline the government agencies the victim may need to deal with (including FMA or OPC responsibilities).
6. Providing targeted introductions to private sector providers – ISPs, MSPs, Bank Fraud, Netsafe, etc.
8. A follow up call back within two days later to check on progress (and further calls as needed).
9. A NPS assessment once they have returned to BAU.

Appendix 3: CERT NZ Mandate

The mandate of CERT NZ in 2022 remains the same as when they were established under the National Cyber Security Strategy 2015 – this being five fold:

1. **Incident response and triage** – taking reports from individuals and organisations, analyse, triage and on-refer.

2. **Situational awareness and information sharing** – sector based info sharing, vulnerability and threat analysis, receive and analyse data feeds.

3. **Advice and outreach** – provide advice on threats/prevention/mitigation, domestic liaison, data reporting.

4. **International collaboration** – liaison with offshore partners and agencies, international organisation membership.

5. **Co-ordination of serious cyber incidents.**

Appendix 4: Lessons and challenges shared by CERT NZ

1. **It takes time to build trust with agencies.** When CERT NZ was established it was a new player in the cyber security landscape, and this meant that it had to establish new relationships and build trust. We would caution against any approach that introduces new agencies into the system, as our experience is that it will take a while for them to be effective.

2. **"Build it and they will come" only gets you so far.** To be an effective reporting and triage agency, you need to be working hand-in-hand with partner agencies. If you build something you hope others will join up and don't require a commitment from other agencies (e.g. a commitment to remove other reporting channels), there are trade-offs:

    - The public continues to get an inconsistent/confusing experience for longer.
    - The time it takes for agencies to decide whether they will shift to a shared platform, and to undertake the necessary legal scrutiny to do this is significant.
    - We consider that Government needs to indicate a clear direction for agencies to follow.

3. **Set a funding roadmap.** Funding for a minimum viable product and with uncertain demand means that the agency will be in a cycle of trying to be funded to undertake its tasks, which takes resourcing away from delivery.

4. **Set a host agency.** Likewise, establishing an agency without clarity on its host agency beyond the first 1-2 years makes it difficult to plan for the medium to long term, and takes focus away from delivery.

5. **Timeframes for new services need to be informed by operational experience.** The pace at which CERT NZ was established mean that some trade-offs were made around reporting and triage design (e.g. there wasn't time in some areas to innovate or request further clarity from Cabinet). If we want the single front door to be transformational, it needs to have the time to build agencies' support and agreement.

Appendix 5: Possible touchpoints between the OPC and SFD

Should the proposed single front door go ahead, the Office of the Privacy Commissioner (OPC) notes that considerable work will need to be undertaken between the SFD as navigator/service channel, and the OPC. Four likely touch points are:

1. At the time a breach occurs – the SFD should refer the "victim business" to OPC to undertake its mandatory breach notification. Should a business come first to OPC, the business should be referred to the SFD to access specialist technical cyber-security support.

2. Reporting on progress with breach response and mitigation.

3. Individuals who contact the SFD for assistance should be made aware of the fact that they can make a complaint to the OPC if they feel that a business has breached their privacy.

4. "Case closure" – it is likely that what defines "case closure" will be different for the SFD and OPC.

Appendix 6: Current government investment

Cyber Security Agency Operational Budgets		
Agency	*Approximate Baseline*	*Note*
CERT	$13.65m	In addition to this baseline funding, we note CERT received additional future-funding in the most recent budget.
DIA	$10.50m	Total B22/23 Appropriation for Digital Safety (includes other non-CS workstreams such as harmful content, community response; and awareness).
NCSC	?	GCSB funding breakdowns are not available publicly.
Netsafe	$4.06m	Figure obtained from 2020/21 Annual Report – note that around three quarters of this funding is for investigating complaints under the Harmful Digital Communications Act.
Police	$2.5m	Estimate from Police Cybercrime.

Source: Public facing agency documentation