



# Aide-Memoire

## AUSTRALIA CYBER SECURITY CENTRE'S ANNUAL CYBER THREAT REPORT (2020-2021)

<b>To</b>	Hon Dr David Clark, Minister for the Digital Economy and Communications	<b>Report No</b>	2122NSP047
<b>From</b>	National Cyber Policy Office, Department of the Prime Minister and Cabinet	<b>Date</b>	27/10/2021

### Purpose

1. This aide-memoire provides a brief summary of the Australia Cyber Security Centre's (ACSC) recently published Annual Cyber Threat Report 2020-2021.<sup>1</sup> It also outlines key similarities and differences to New Zealand's analysis of the cyber security threat landscape, drawing on statistics and trend observations from the NCSC and CERT NZ.

### Background

2. The ACSC Annual Cyber Threat Report 2020-2021 was released on 15 September. It is the second unclassified annual cyber threat report that the ACSC has produced.
3. The report was produced by the ACSC, with contributions from the Defence Intelligence Organisation (DIO), Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO), the Department of Home Affairs, and industry partners.
4. The report highlights six key cyber security threats identified as having had a significant impact on Australia over the 2020-2021 financial year:
  - Exploitation of the pandemic environment
  - Disruption of essential services and critical infrastructure
  - Ransomware
  - Rapid exploitation of security vulnerabilities
  - Supply chains
  - Business email compromise
5. It also provides trends analysis and case studies that describe the nature and scope of threats and recommends measures for Australian citizens and businesses to protect their systems against cyberattacks.

<sup>1</sup> <https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>

---

### *Key statistics from the Report*

6. There has been a 13% increase in reported cybercrime in Australia from the previous financial year, with self-reported losses totalling more than AU\$33 billion.
7. Approximately one quarter of reported cyber security incidents affected entities associated with Australia's critical infrastructure.
8. Over 1,500 cybercrime reports per month of malicious cyber activity were related to the coronavirus pandemic.
9. The average severity and impact of reported cyber security incidents has increased, with nearly half categorised as 'substantial'.

### **Comment and comparison with New Zealand**

---

10. As New Zealand and Australia measure and report slightly different statistics, it is difficult to do a direct comparison, but the threat trends outlined in the ACSC report are nevertheless broadly the same as those observed both domestically and globally over the last year. This reflects the ongoing changes in the cyber security environment being driven by global trends.
11. The exploitation of the COVID-19 pandemic environment by cybercriminals is the most significant change in the overall cyber security environment. Due to a heightened dependence on the internet, and especially during periods of state-wide or national lockdown, both Australia and New Zealand have recorded a significant increase in cyberattacks.
12. The pandemic has also accelerated the migration of many businesses on both sides of the Tasman to e-commerce and digital services. Many businesses, particularly SMEs, have made this transition without understanding or adoption of good cyber security practices, therefore increasing their vulnerability to cyberattacks.
13. In parallel, both countries have experienced an increase in attacks affecting critical infrastructure. ACSC has reported that approximately one quarter of cybercrime incidents affected organisations associated with critical infrastructure and, in particular, the Australian healthcare system has been targeted by both state actors and independent criminal groups. Increased activity by state actors is cited as likely motivated by the theft of intellectual property or sensitive information pertaining to Australia's COVID-19 response, and by criminal groups motivated by a higher likelihood that a victim may pay a ransom if an essential service is jeopardised. New Zealand has experienced similar debilitating attacks, such as those on the Waikato District Health Board, which disrupted the operations of several hospitals, and the Department of Conservation's search and rescue base at Aoraki/Mt Cook.
14. Ransomware continues to be a rampant issue worldwide, growing in profile and impact. The ACSC recorded 500 reported ransomware incidents from 2020-2021, a 15% increase from the previous financial year. For the Q2 period 1 April to 30 June 2021, CERT NZ received 30 reports of ransomware, a 150% increase over the previous quarter.
15. Both countries have also seen a noticeable change in the modus operandi of these attacks over the 2020-2021 period. Namely, recent ransomware attacks have increasingly targeted larger companies or critical services, causing widespread impact and severe disruption. In addition, ransom demands tended to be higher, and the malware used more sophisticated. The effects of recent ransomware attacks on large businesses like New Zealand's Lion Breweries and Fisher and Paykel, and Australia's Toll Group were felt on both sides of the Tasman. The cross-border implications of these attacks further underscore the importance of international cooperation (a cyber security priority for both countries) in combatting cybercrime



going forward. CERT NZ engages closely with its Australian and international counterparts, sharing information and mitigation measures to address ransomware issues.

16. The exploitation of publicly reported or zero-day vulnerabilities is a key vector used by large-scale international campaigns to deploy ransomware or exfiltrate data. Although not specifically targeted, New Zealand and Australian organisations have been indirectly impacted by extortion campaigns like the exploitation of the Microsoft Exchange server vulnerability in March 2021 and the Kaseya ransomware attack which compromised the data of 11 New Zealand schools.
17. Australia's reporting provides a comprehensive breakdown of cybercrime data. The ACSC report provides insights into scam trends such as a rise in the impact of business email compromise scams. The average loss per successful business email compromise has increased to more than \$50,600 (AUD) – over one-and-a-half times higher than the previous financial year. Fraud, shopping and online banking scams continue to be the dominant forms of cybercrime in Australia, collectively making up 52% of all reported incidents, and emphasising how the pandemic has provided compelling content for email and SMS phishing campaigns.
18. CERT NZ trend analysis reflects a steady 15-20% rise in reported incidents and losses year-on-year, with malware, ransomware, phishing and scam incidents becoming more prevalent as businesses and New Zealanders rapidly adopt digital technology. Corresponding to New Zealand's heightened digitisation, reports of cryptocurrency investment scams have also become more common, increasing by 50% from the last quarter.
19. The rise in the financial impact of cybercrime has been captured in both the ACSC report and CERT NZ reporting. CERT NZ reported \$3.9 million (NZD) in financial losses in quarter 2 in 2021, a 30% increase from Q1, with financial losses from \$10K to >\$100K (NZD) per incident becoming more commonplace. In Australia, self-reported financial losses due to cybercrime totalled more than \$33 billion (AUD) in 2020-2021, with medium sized businesses reporting the highest losses per incident.
20. Finally, the ACSC report mirrors New Zealand agencies' calls for individuals to exercise better basic cyber hygiene, and for businesses to see the value in investing to secure their networks. The report offers resources and advice on how individuals or businesses can protect themselves from attacks by utilising basic tools and practices like strong passwords, multifactor authentication, and regular back-ups.
21. A 2020 survey conducted by CERT NZ showed only 34% of SMEs had a reasonably good understanding of cyber security practices. A rolling set of awareness-raising campaigns involving government agencies and private sector organisations continue to focus on practical management of cyber security. CERT NZ's Cyber Smart Week is an example of this.
22. The NCSC Annual Cyber Threat Report 2020-2021 is scheduled to be published before the end of 2021
23. Many of the issues raised above are being considered and addressed in a New Zealand context through implementation of the Cyber Security Strategy, as well as through options which will be presented through the November and March reports-back to Cabinet on strengthening cyber security and resilience in the public and private sectors. In addition, agencies including CERT NZ and the NCSC work directly to prevent and address attacks on critical infrastructure and SMEs, to counter malware, ransomware, phishing attacks, and scams, and to raise cyber security awareness.

## Recommendations

---

24. It is recommended that you note the contents of this aide-memoire.

Tony Lynch  
Deputy Chief Executive  
National Security Group

NOTED

Hon Dr David Clark  
Minister for the Digital Economy and Communications

Date:    /    /

Released under the Official Information Act 1982





# Aide-Memoire

## CYBER SECURITY STRATEGY IMPLEMENTATION – WORK PROGRAMME UPDATE

<b>To</b>	Minister for the Digital Economy and Communications (Hon Dr David Clark)	<b>Report No</b>	2122NSP/054 DPMC-2021/22-604
<b>From</b>	National Cyber Policy Office, Department of the Prime Minister and Cabinet	<b>Date</b>	8/11/2021

### Purpose

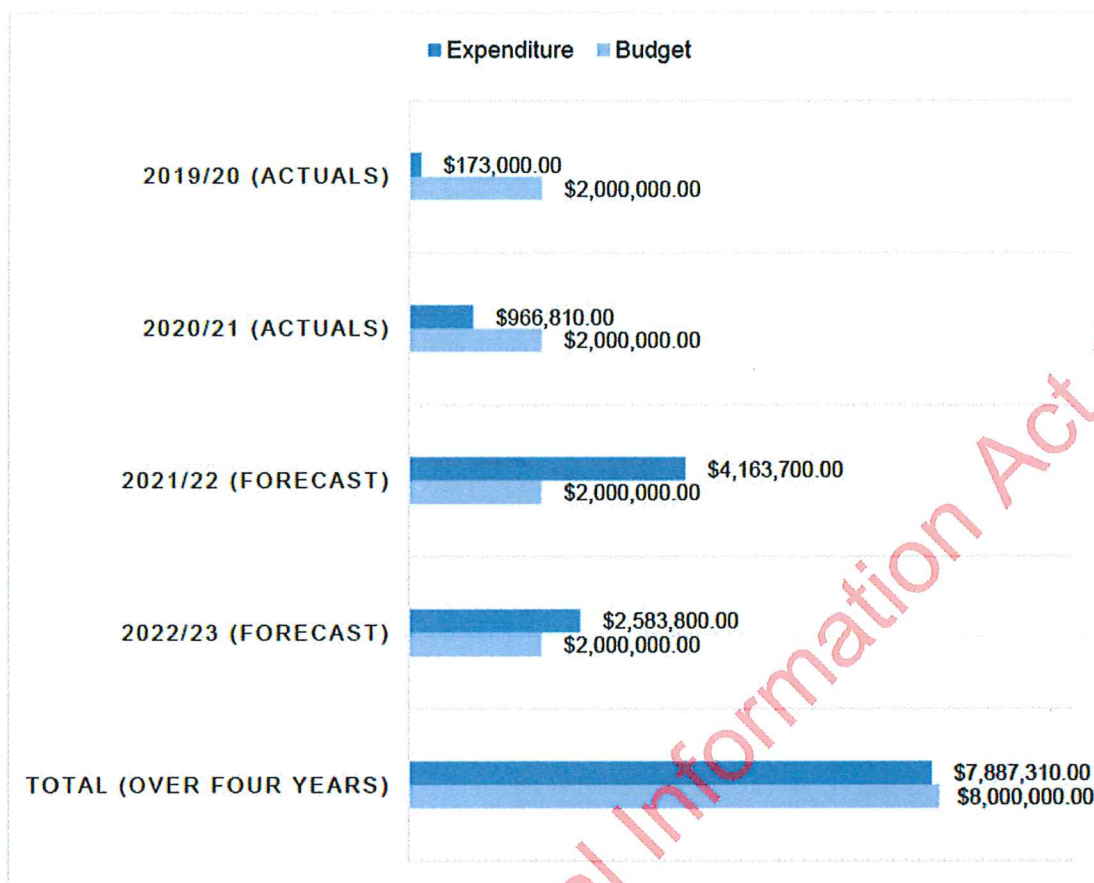
1. To provide an update, as requested, on the implementation of the Cyber Security Strategy work programme, comprising expenditure to date and proposed future projects through to 2022/23.

### Background

2. Budget 2019 delivered \$2 million per financial year on an ongoing basis for the implementation of the Cyber Security Strategy.
3. This is additional to other cyber security funding across government (such as the baseline funding for the Government Communications Security Bureau's (GCSB) National Cyber Security Centre (NCSC), CERT NZ, NZ Police's work against cyber criminals, and departmental IT expenditure).
4. The funding is used for joint-agency projects to enhance national cyber security at a system level. Projects and initiatives funded through the strategy implementation are focused on aspects of the Strategy priority areas that are not well addressed by other government expenditure.
5. The Department of the Prime Minister and Cabinet (DPMC) is the administering agency. Individual projects may be project-managed by other agencies.

### Comment

6. The total appropriation out to 2022/23 is \$8,000,000 (i.e. \$2 million per financial year, for four years). Current projected expenditure on projects for the four year period totals \$7,887,310 as represented in the table below. Any residual will be applied to future projects (refer paras 14-15 below).



#### Breakdown of expenditure to date

7. As previously advised (2021/NSP/022), the impacts of COVID-19 have resulted in aspects of the Strategy implementation being delayed or deferred.
8. For the current financial year of 2021/22, the total budget for implementation is \$4,860,190. This includes \$2,860,190 expected to be carried forward from 2019/20 and 2020/21.
9. The year to date spend for 2021/22 is \$109,000 (as at 30 September – additional invoices for projects underway are expected to be received and paid out by DPMC in the coming months).

#### Projects funded under the Strategy as at October 2021

10. The following items have either received funding or had funding approved from the Cyber Security Strategy appropriation. Lead agencies are listed in brackets.

Project	Cost
Cyber security market research on behaviours to inform awareness campaigns (through to 2025) (CERT NZ)	\$333,300
GPAI Secretariat contribution (DPMC) (over 3 years, to 2022/23)	\$237,400
Trade Smart campaign contribution (CERT NZ)	\$200,000
Translation of CERT NZ advice into commonly spoken languages (CERT NZ)	\$250,000
Women in Cyber international workshop contribution (MFAT)	\$42,000



Salaries and other operating costs, including for the Christchurch Call Unit (DPMC) <sup>1</sup>	s9(2)(a)
<b>Total</b>	s9(2)(a)

**Planned projects for 2021/22 and 2022/23**

11. The following items are projected to be funded from the appropriation in 2021/22 and 2022/23, and some are close to or already progressing (but as they have not yet been invoiced they are not included in the list above). Lead agencies are listed in brackets.

Proposed project	Cost
s9(2)(f)(iv)	
Industry competitiveness plan (DPMC)	\$200,000
s9(2)(f)(iv)	
Cyber Security Workforce Research Project (DPMC)	\$240,000
s9(2)(f)(iv)	
<b>Total</b>	<b>\$2,814,000</b>

12. From 2021/22, the salaries of 4.8 FTEs are funded from the appropriation to better deliver the Strategy, s9(2)(a). These FTEs have enabled the delivery of high priority workstreams, including the extensive policy work and Māori engagement to support New Zealand's accession to the Budapest Convention, as well as work on cyber security workforce development, and industry growth.

13. In addition, the contribution to the Christchurch Call Unit supports 3.6 FTEs (MFAT also provides FTEs to the unit).

**Future projects**

14. You requested advice on the establishment of an independent Cyber Security Advisory Committee (CSAC) [as outlined in 2122NSP/051]. As proposed, the Strategy implementation fund would provide \$85,000 for the CSAC for a six-month period. A proposal on this is being submitted to the Strategy governance committee for approval, and will then require sign off from the Chief Executive of DPMC.

<sup>1</sup> This includes funding over the following financial years 2019/20, 2020/21, 2021/22 and 2022/23.

<sup>2</sup> If required for a consultant to look at Māori oversight/review function.

<sup>3</sup> Work on hold while NCPO supports the development of the Cyber Security Advisory Committee.

15. s9(2)(f)(iv)



**Recommendations**

16. It is recommended that you note the contents of this aide-memoire.

NOTED
<p>Hon Dr David Clark  <b>Minister for the Digital Economy and Communications</b></p>
<p>Date:     /     /2021</p>

Tony Lynch  
**Deputy Chief Executive  
National Security Group**

Date: 08/11/2021

Released under the Official Information Act 1982





# Aide-Memoire

## INTERNATIONAL PARTNERS' CYBER SECURITY POLICY AND STRATEGY DEVELOPMENTS

To	Hon Dr David Clark, Minister for the Digital Economy and Communications	Report No	2122NSP/049
From	National Cyber Policy Office	Date	9/11/2021

### Purpose

1. This aide-memoire provides a summary of recent cyber security policy and strategy developments in Australia, the United States, and the United Kingdom.

### Background

*Australia's Security Legislation Amendment (Critical Infrastructure) Bill 2020*

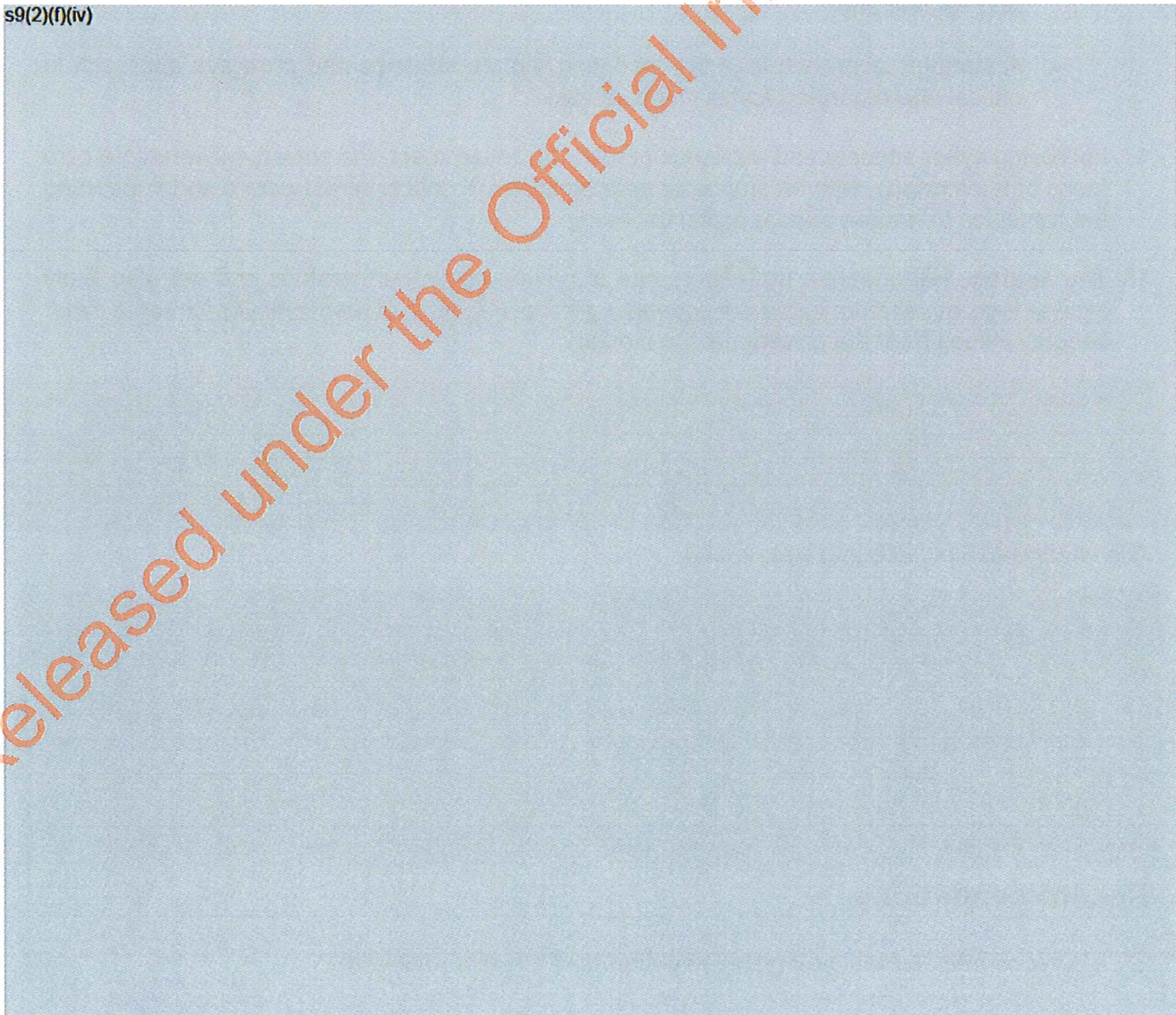
2. The Critical Infrastructure Bill currently progressing through parliament aims to enhance the existing framework for managing risks relating to critical infrastructure. Upon recommendation from the Federal Parliament's Joint Committee on Intelligence and Security (PJCIS), the Australian government has now split the bill into two parts. According to the Minister for Home Affairs, splitting the bill in half will fast-track the passage of urgent reforms to ensure the security of the country's critical infrastructure, while allowing more time for less urgent aspects of the bill to be consulted and designed in partnership with industry stakeholders.
3. The expedited reforms include requiring critical infrastructure operators to report cyberattacks within 12 hours of discovery and granting the Australia Signals Directorate power to intervene in the event of a significant incident to protect targeted networks. The urgent, standalone bill also covers the redefinition of what is considered "critical infrastructure", which has been updated following the Security of Critical Infrastructure Act 2018 to include universities, finance and banking, health and the food and grocery sectors, communications, defence industry, energy, and transport.
4. The PJCIS has advised, however, that there are parts of the bill that are intended to be co-designed with stakeholders and therefore require more in-depth engagement with operators and providers. Splitting the urgent and non-urgent elements of the bill will give the government the readiness to respond to the immediate threat of a cyber attack, while still allowing for a thorough consultation process to take place prior to developing long-term security measures and regulatory frameworks.



*The United States' Cyber Incident Reporting Act*

5. On 28 September, U.S. Senators on the Homeland Security and Governmental Affairs Committee introduced the Cyber Incident Reporting Act. The bipartisan legislation requires operators and providers of critical infrastructure to report cyber attacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of the breach.
6. Additionally, organisations with over 50 people, non-profits, and local and state government agencies would need to notify CISA within 24 hours if they make a ransom payment and ensure they have carefully evaluated all other alternatives before making the decision to pay.
7. The bill includes enforcement mechanisms which are built into the legislation. It provides CISA with the authority to subpoena entities that fail to report cyber security incidents or ransomware payments and warns that entities that fail to comply with the subpoena can be referred to the Department of Justice and barred from contracting with the federal government.
8. Finally, the bill mandates an interagency ransomware taskforce. The taskforce is intended to facilitate whole-of-government responses to major attacks on the country's critical infrastructure. The announcement follows several high-profile ransomware attacks including the Colonial Pipeline incident in May that caused the company to shut down thousands of miles of pipeline, causing gas price gouging and shortages along the eastern coast, and even impacting flight schedules.

s9(2)(f)(iv)





*The United Kingdom's Cyber Strategy*

14. Following the release of the UK's Integrated Review of Security, Defence, Development and Foreign Policy in March, work began on a refreshed cyber strategy, scheduled for publication before the end of the year (the UK's current National Cyber Security Strategy 2016-2021 expires this year).
15. The Integrated Review called for the UK to invest in developing the country's competitive edge as well as its cyber defences. To that end, the new cyber strategy will broaden the focus from pure 'cyber security' to a more comprehensive national cyber strategy. The widened scope is intended to go further than protecting against and responding to cyber threats and will include work to develop offensive cyber capabilities and strengthen the UK's international influence.
16. The strategy will comprise four broad pillars, underpinned by a cross-cutting programme of work focused on bolstering the wider UK cyber ecosystem:
  - Resilience – building the UK's domestic cyber security capacity;
  - Mitigating threats – detecting, disrupting and deterring threat actors, including by taking actions to impose costs;
  - International influence – shaping the global cyber environment in line with UK interests and values; and
  - A strategic approach to tech – adopting a more strategic and proactive approach to critical and emerging (cyber) technologies.
17. Improving cyber security and resilience across UK government and society will remain a core focus of the strategy, with an emphasis on protecting UK critical infrastructure and supporting the transition to a more secure digital economy.
18. The strategy will underpin the importance of private-public partnerships and will also likely include legislative reforms that will support a gradual transition of responsibility for some cyber security issues from the government to industry.

s6(a)


*Alignment with New Zealand's approach*

s9(2)(f)(iv)

---

## Recommendations

21. It is recommended that you **note** the contents of this aide-memoire.



Halia Haddad  
Manager, National Cyber Policy Office  
Department of the Prime Minister and  
Cabinet

Date: 09 / 11 / 21

NOTED
<p>Hon Dr David Clark Minister for the Digital Economy and Communications</p>
Date: / /

Released under the Official Information Act 1982





# Digital Economy and Communications aide memoire

Hon Dr David Clark  
Minister for the Digital Economy and Communications

Title: **Decommissioning and recycling Government agency devices**

Date: 10 November 2021

## Key issues

This Aide Memoire provides advice on work to explore the potential for redistributing decommissioned government agency devices to digitally excluded New Zealanders.

## Action sought

Note the advice in this Aide Memoire.

## Timeframe

N/A

## Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1 <sup>st</sup> contact
Adrienne Moor	Strategic Advisor, System Strategy and Initiatives	021 847 205	✓
Colin Holden	General Manager System Strategy and Initiatives	027 210 2568	

Return electronic document to:	Catherine.McGregor@dia.govt.nz
Cohesion reference	4UAZY7VS6QRJ-242273383-1167
Ministerial database reference	DEC202100388

For Minister's office:	<input type="checkbox"/> Seen	<input type="checkbox"/> Approved	<input type="checkbox"/> Declined	<input type="checkbox"/> Withdrawn	<input type="checkbox"/> More information required
------------------------	-------------------------------	-----------------------------------	-----------------------------------	------------------------------------	--

## Purpose

1. This briefing updates you on work the Digital Public Service branch has commenced, initially with the Ministry for Business, Innovation and Employment (MBIE), to explore the potential to recycle decommissioned government agency devices for provision to digitally excluded New Zealanders.

## Background

2. Approximately 50,000 devices owned by government agencies reach the end of their life cycle each year. The length of life cycle varies from agency to agency, but devices would normally be replaced after three years' use. Agencies currently have different approaches to dealing with their redundant devices, which may range from decommissioning for re-sale or donation to simply wiping and disposing of the devices. There may be an opportunity ultimately to bring agencies under an all-of-government decommissioning framework.
3. Under the current model, when devices reach the end of their life cycle, they are provided to a commercial recycling company to be decommissioned and prepared for re-sale. Decommissioning involves securely transferring and or wiping content from the hard drive and restoring factory settings on each device. MBIE is currently in the process of renegotiating its commercial contract for this decommissioning and re-sale process with the service providers.
4. During your 18 October meeting with representatives of the New Zealand digital technology sector, Victoria MacLennan, co-Chair, NZRise and Chair of Digital Future Aotearoa Charitable Trust, identified an opportunity for re-purposing decommissioned government agency devices for digitally excluded New Zealanders.

## Comment

5. There is potential to consider an all-of-government approach to re-purposing decommissioned government agency devices for New Zealanders who do not have access to devices of their own. This could become part of an integrated, multi-year, cross-agency work programme aimed at improving digital inclusion currently being developed under the Digital Strategy for Aotearoa umbrella. This approach would also go some way to meeting expectations of responsible whole-of-life stewardship of government owned electronic devices.
6. Re-purposing devices to meet digital inclusion needs is not a straightforward issue, and some detailed research and analysis will be required to progress this work. As a first step, we intend to explore feasibility issues and options for reallocating devices with some support from MBIE.
7. MBIE has advised it could be in a position to work with us on these issues early in the New Year.

## Points to note

8. There are a number of issues that need to be considered as part of this exploratory work. These include:
  - 8.1 Re-distribution model – should the re-purposed devices be provided free of charge to digitally excluded New Zealanders, or sold at a discounted price? If sold, how would they be priced?



- 8.2 Does the commercial decommissioning model allow recycled devices to be donated to individuals rather than re-sold? How does this align with government procurement processes?
- 8.3 The state of the device at the end of its life cycle – is it fit for repurposing for digitally excluded New Zealanders?
- 8.4 The value of a device at the end of its life cycle – noting that the cost of a government agency device would be fully depreciated after three years. Are there ownership issues to consider?
- 8.5 Security issues around sensitive information potentially retained on the devices– is wiping of the hard drive as part of the decommissioning process sufficient to address these?

9. s9(2)(f)(iv) [Redacted]

10. We will report back to you with further information, once the exploratory work with MBIE is underway.

  
**Ann-Marie Cavanagh**  
Deputy Government Chief Digital Officer

Released under the Official Information Act 1982



# Aide-Memoire

## CONFLICT OF INTEREST DECLARATIONS – CYBER SECURITY ADVISORY COMMITTEE

<b>To</b>	Hon Dr David Clark, Minister for the Digital Economy and Communications	<b>Report No</b>	2122NSP/104
<b>From</b>	Tony Lynch, Deputy Chief Executive, National Security Group	<b>Date</b>	22/12/2021

### Purpose

1. This note provides advice that appropriate conflict of interest enquiries have been undertaken for the members of the Cyber Security Advisory Committee (CSAC), in line with the Terms of Reference of the Committee and drawing on advice from DPMC Corporate Legal Services. These enquiries have not identified any areas of concern.

### Recommendations

1. It is recommended that you **note** that appropriate conflict of interest enquires for the members of the Cyber Security Advisory Committee (CSAC) have now been completed as outlined in Attachment A and have not identified any areas of concern.

Tony Lynch  
Deputy Chief Executive,  
National Security Group  
Department of the Prime Minister and  
Cabinet

Date: 23 / 12 /2021

NOTED

Hon Dr David Clark  
Minister for Digital Economy and  
Communications

Date: / /2021





**Attachment A: Summary of conflict of interest enquiries**

Name of member	Conflicts of interest identified (as described by member)	Proposed management plan	Comment from DPMC Corporate Legal Services
s9(2)(a)	[Redacted]	Reviewed – no concerns	Reviewed – no concerns
		Reviewed – no concerns	Reviewed – no concerns
		Reviewed – no concerns	Reviewed – no concerns

Released under the Official Information Act 1982



~~IN CONFIDENCE~~

s9(2)(a)

Reviewed – no concerns



Released under the Official Information Act 1982

~~IN CONFIDENCE~~



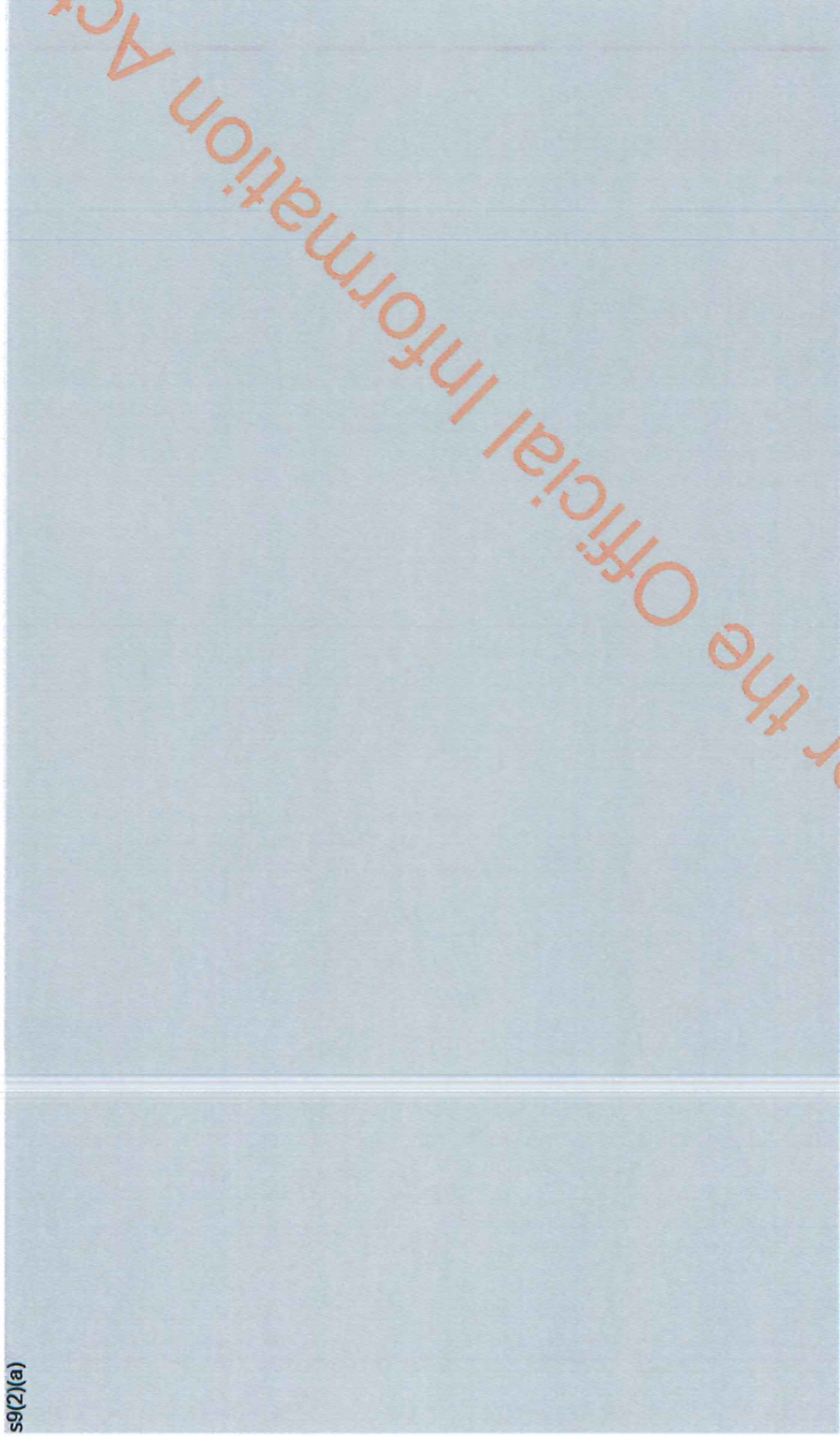
s9(2)(a)

While the detail provided on this form is minimal, the member gave more detailed information in her candidate form and has proposed acceptable mitigations in the event of a conflict arising. Based on that information, DPMC Legal considers we have enough assurance to know that the member will act appropriately in the event a conflict does arise.

Reviewed – no concerns

Reviewed – no concerns

Reviewed – no concerns



Released under the Official Information Act 1982



# Briefing

## SECURING THE INTERNET OF THINGS IN NEW ZEALAND

To Minister for the Digital Economy and Communications and Minister of Commerce and Consumer Affairs (Hon Dr David Clark)

Date	25/01/2022	Priority	Medium
Deadline	<a href="#">Click here to enter a date.</a>	Briefing Number	2021/22-962

### Purpose

This briefing provides an overview of the Internet of Things (IoT) and the cyber security implications of the increasing use of IoT devices in New Zealand. It seeks your agreement to focus on developing security policy options for consumer smart devices, s9(2)(f)(iv)

### Recommendations

1. Note that IoT is a growing vector for cyber attacks, and the security of IoT devices is an integral part of building New Zealand's overall cyber resilience;

2. Agree that initial policy options for IoT security should focus on consumer smart devices;

YES / NO

3. s9(2)(f)(iv)



4. Refer this briefing to the Ministers responsible for National Security and Intelligence; the Government Communications Security Bureau; Research, Science and Innovation; Trade; and Small Business.

<p>Tony Lynch  <b>Deputy Chief Executive,                  National Security Group</b></p>	<p>Hon Dr David Clark  <b>Minister for the Digital Economy and                  Communications</b></p> <p><b>Minister of Commerce and Consumer                  Affairs</b></p>
<p>25/01/2022</p>	<p>...../...../.....</p>

**Contact for telephone discussion if required:**

Name	Position	Telephone		1st contact
Halia Haddad	Manager, National Cyber Policy Office	DDI: s9(2)(a)	Mobile: s9(2)(a)	✓
s6(a)	Policy Advisor, National Cyber Policy Office	DDI: s9(2)(a)	Mobile: s9(2)(a)	

**Minister's office comments:**

1. Noted
2. Seen
3. Approved
4. Needs change
5. Withdrawn
6. Not seen by Minister
7. Overtaken by events
8. Referred to

# SECURING THE INTERNET OF THINGS IN NEW ZEALAND

## Purpose

---

1. This briefing provides an overview of the Internet of Things (IoT) and the cyber security implications of the increasing use of IoT devices in New Zealand. It seeks your agreement to focus on developing security policy options for consumer smart devices, s9(2)(f)(iv)

## What is the Internet of Things?

---

2. IoT refers to the billions of internet-connected devices around the world that collect and share data. The term IoT is mainly used for devices that have not traditionally had an internet connection, and that can communicate with a network of other IoT devices independently of human action. Smartphones and personal computers are not generally considered IoT devices.
3. IoT devices are being increasingly integrated into consumer's lives and commercial and industrial sectors, including homes, critical infrastructure, vehicles, medical devices, and form the basis for smart cities. Utilities and agricultural sectors have had significant uptake of IoT devices to streamline business operations and more readily detect service disruptions in critical economic and infrastructure areas.
4. The addition of sensors has provided IoT devices a level of digital intelligence, enabling them to collect and communicate data in real time, to be more responsive and to improve service delivery and resource management. Their ability to store and utilise large amounts of data can streamline processes and create increasingly efficient services. As the uptake of IoT devices increases, this will likely see benefits and solutions across multiple sectors.
5. There are three broad categories of IoT devices:
  - *Consumer and personal smart devices:* There are a broad range of consumer and personal smart devices. Devices such as FitBits are having positive impacts on health through monitoring data and providing feedback on individuals' health and daily habits. Smart home devices such as smart lighting and alarm systems provide efficiency, convenience, and cost savings for consumers;
  - *Industrial IoT devices:* These devices are embedded into industrial systems. For instance, in the utilities sector, smart quality water systems monitor water storage levels and flow, detect and locate leaks, and forecast demand. This can contribute toward mitigating the effects of climate change and population growth on water supply; and
  - *Enterprise IoT devices:* These devices are included in objects and machines to participate in business processes involved in the likes of smart buildings and offices. This provides more tailored experiences for individuals, reduces manual work and increases efficiency and productivity.
6. The rollout of 5G networks is likely to accelerate the adoption of IoT devices by enhancing their capability and performance through the increased data transfer and operating speeds,



and the greater network bandwidth that 5G offers. 5G networks can handle many more connected devices which, in turn, are able to operate at faster speeds (up to ten times faster) than 4G networks.

## IoT comes with risks

---

7. While there are many potential benefits from the use of consumer, industrial and commercial IoT devices, there are also a range of cyber security risks. Many of these devices have not been designed or deployed with security in mind, and therefore provide multiple potential entry points for cyber attacks.

### *Security of IoT devices*

8. IoT devices are vulnerable when:
- Manufacturers do not embed security into their devices. Cheap and quick production is often favoured to maximise short-term profit;
  - Security updates are few and far between (if there are updates at all) given the economics of manufacturing supports large scale productions with short life span-product lifecycles, compared with a longtail of the life of installed devices;
  - One of the multiple access points to a network is left exposed. The greater number of devices attached to a network, the more entry points there are for a malicious actor to gain access to a network. This is exacerbated when security protections are not factored into the design of a device;
  - Users do not change default usernames and passwords on devices, allowing threat actors to use recycled credentials to gain access to a network of devices; and
  - Internet-connected networks are compromised (IoT devices operate on these networks).
9. The lack of security of IoT devices presents serious economic, privacy, and safety risks, as they are increasingly integrated into individuals lives and homes and commercial and industrial supply chains and processes. There are also potential national security implications as a result of the integration of potentially insecure devices into critical infrastructure.



**The Mirai Botnet**

*Mirai is a malware that is used to infect IoT devices. The malware takes remote control of multiple IoT devices, creating a botnet. The botnet can then be used to perform activities such as a distributed denial of service (DDoS) attack which makes devices and networks unavailable.*

*The Mirai botnet exemplifies the risk insecure IoT devices present. In 2016, hackers scanned the internet for IoT devices, including security cameras and wireless routers, that still used typical default passwords. Using these passwords, hackers infected and gained access to up to 600,000 devices at its peak.*

*Mirai created a botnet of compromised IoT devices and launched a DDoS attack which brought down popular sites such as Twitter, the Guardian, Netflix, Reddit and CNN. This slowed or stopped the internet for nearly the entire eastern United States making it the largest attack of its kind.*

*The catch: the brains behind the Mirai botnet were three 21-year-old college students who had been trying to gain an advantage in the computer game Minecraft and unintendedly brought down the internet. This highlights the potential national security risk that insecure IoT devices could present when under the control of a well-resourced state actor.*

10. Although insecure IoT devices can be easily compromised, manufacturers and retailers of these devices rarely bear the costs or experience the harms. This means that the potential risks of insecure devices are not factored into decisions relating to their design, manufacture, or sale.

*Consumer protection and awareness*

11. Vast amounts of data on consumers and their homes is collected and processed by their smart home and personal smart devices. The processing of this data enhances the services provided by IoT devices. However, in many markets (including in New Zealand) there is a lack of information available to consumers at the point of purchase on the security of a device and the type of data used to streamline processes. The potential impacts of a compromise for consumers include:
  - Exposure of personal information including health and financial data;
  - Breaches of privacy through providing access to various accounts and devices that may have camera and audio capabilities;
  - Revealing of private information on a consumer's home and family through smart home networks; and
  - Physical harm due to the increasing evolution and utilisation of technology such as remote medical devices and autonomous vehicles.
12. Consumers bear most of the risk when they unknowingly purchase insecure and poorly-supported IoT devices. They also have few ways to differentiate between poorly-secured IoT devices and their more secure equivalents to make informed purchasing decisions.
13. The economics of some manufacturing do not favour products with long lifecycles that are well-supported through security updates. This means that there is a constant supply of IoT devices that are less secure with short-product lifecycles available to consumers.



**Hacking of Amazon's smart doorbells**

The Amazon-owned company Ring manufactures smart home security products such as outdoor motion-detecting cameras and Smart doorbells.

In 2019 Hackers breached connected doorbells and home monitoring systems using recycled credentials. The hackers were able to access live feeds from the cameras around the Ring customers' homes, and verbally harassed families using the devices' integrated microphones and speakers. Complaints were filed by more than 30 people in 15 families who say their devices were hacked and used to harass them.

This example demonstrates the risk that is faced by consumers when they integrated insecure devices into their homes.

14. There is currently no incentive or economic reason for manufacturers to build security into the design of IoT devices. Additionally, there is no transparency of the device's level of security to help mitigate the risk that exists for consumers.

**IoT in New Zealand – the case for change**

*Current IoT usage in New Zealand*

15. IoT devices are already being integrated into domestic and commercial networks throughout New Zealand's society and economy. New Zealanders are also more readily integrating IoT devices into their lives and homes.
16. New Zealand has a particularly large uptake of IoT devices in the AgriTech sector. The devices are used to monitor irrigation and livestock to make farming practices more efficient. Streamlining agricultural processes in this way could see large benefits for the New Zealand economy.
17. New Zealand is largely a technology-taker and user in the IoT market, particularly with consumer IoT devices and services. However, we do have a small number of businesses that manufacture and sell niche commercial and industrial IoT devices and services.
18. The adoption and use of IoT devices will likely increase alongside Spark NZ's plans to invest an additional \$35 million (totalling \$125 million) into their 5G rollout. The investment will provide 90% of the population with 5G access by the end of 2023, the uptake and use of which will add, in Spark NZ's estimation, \$5.7 – \$8.9 billion to the New Zealand economy over the next ten years.

*New Zealand's IoT threat landscape*

19. According to CERT NZ's Q3 2021 report, attackers continue to hack and use networks of IoT devices (a botnet) to launch DDoS attacks. Using data from Shadowserver Foundation, CERT NZ also identified that there were over 1,300 attacks in October 2021 alone resulting from malicious actors accurately guessing passwords to access online accounts and IoT devices.
20. There are some protections for consumers in New Zealand that apply to IoT devices (amongst other things). These include:



- *The Privacy Act 2020*: The Act states that an organisation with a presence in New Zealand must notify the Office of the Privacy Commissioner of data breaches. This would apply to data from IoT devices. If the organisation involved in the loss of the data is based overseas the reporting requirements may be difficult to enforce.
  - *The Consumer Guarantees Act*: The Act sets out that goods supplied to a consumer must be of acceptable quality, and requires manufacturers to take reasonable action to ensure that facilities to repair goods are available for a reasonable period. However, there are no specific provisions in the Act that might apply to the security of IoT devices.
  - *The Fair Trading Act*: The Act prohibits false and misleading representations regarding the supply of goods or services.
  - *The Telecommunications Act*: Section 108 allows network operators to set standards and manage who (or what) connects to their networks, allowing operators to provide a gatekeeping mechanism for poorly supported or compromised devices. The application of the Act to IoT devices would require further assessment.
21. There are currently no guidelines (voluntary or mandatory) to support or ensure the security of IoT devices in New Zealand. As a net importer of IoT devices, New Zealand is currently fully reliant on IoT security regimes being implemented overseas. While these regimes are useful in lifting the security of IoT devices, it does leave a gap in our current approach that needs to be bridged.
22. Public submissions from consultation on the Digital Strategy confirmed that there is currently an appetite from industry for government to develop 'guidrails' to assist in this area.

### **International approaches to IoT security**

---

23. The approaches other nations have taken to IoT security include:
- *The adoption of, or alignment to one or more international standards*: Standards provide guidance for manufacturers to use in the development of devices, for instance to ensure security is built into the design. Examples of specific priority requirements encompassed in standards include the banning of default passwords; implementing vulnerability disclosure policies for products; and transparency regarding the length of time that a product will receive important security updates.
  - *Consumer labelling schemes*: Labelling schemes indicate a device's level of cyber security to consumers (similar to the energy star rating system, for instance). The information displayed on the label varies, but may include: the 'expiry date' or length of time that security updates will be provided for the device; the level of a particular cyber security standard that the device meets; and how long a label or rating is valid for.
  - *A combined approach of the above*: Many countries use international standards to certify the level of cyber security, which is then presented through a consumer labelling scheme.
  - *These approaches have been implemented through voluntary and mandatory measures*: Many nations have opted to introduce voluntary measures in the first instance, followed by mandatory requirements. Others have allocated voluntary or mandatory measures dependent on the type of IoT device and the risk it poses.



24. The approaches are aligned to three different types of IoT devices. These include:
- Consumer smart devices - devices that are available to everyday consumers including personal and home smart devices.
  - Critical/high risk devices - devices identified as critical/high risk are those that are likely to have greater consequences to the broader network if compromised. Wi-Fi routers and smart home hubs have previously been identified as critical/high risk devices by nations.
  - All smart devices - these include all devices that have the capability of being connected to other IoT devices or a network of IoT devices.
25. New Zealand has engaged with the UK, Singapore and Australia to understand their respective approaches to IoT security. These approaches include:
- **The UK** developed a Voluntary Code of Practice for consumer smart products aligned to an international standard<sup>1</sup>. The Code of Practice introduced 13 requirements for consumer IoT devices that primarily applied to device manufacturers. The UK is now in the process of mandating three specific priority security requirements, which are drawn from the standard. Manufacturers, or importers and suppliers of consumer smart products are responsible for meeting these requirements and ensuring this information is made transparent to consumers.
  - **Australia** initially adopted a Voluntary Code of Practice for consumer smart devices, aligned to the UK version. They are now introducing a consumer labelling scheme, following consultation on options to strengthen Australia's cyber security regulations and incentives. The label will display the time that security updates will be provided for the device. The scheme will apply to all involved in the manufacturing and supply of a product to ensure collective responsibility (rather than assigning one person or point in the supply chain as being most responsible). s6(b)(i)
  - **Singapore** released the IoT Cybersecurity Guide which is aligned to multiple international security standards. The Guide is used to accredit IoT devices to its accompanying Cybersecurity Labelling Scheme. The labelling scheme is mandatory for critical devices (which include smart home hubs and Wi-Fi routers), and optional for all other IoT devices.
26. Throughout these international engagements, our partners have highlighted the alignment of standards or labelling as essential for international interoperability and optimisation of efforts to lift the overall security of IoT devices, and ensure consistent expectations of designers, manufacturers, importers, and suppliers of devices.

### **Proposed approach to IoT security in New Zealand**

27. The security of IoT devices, and the protection of consumers who are well-informed and risk aware, have been identified by officials as two key problems that need to be addressed.

<sup>1</sup> ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements.



28. While ultimately there may be a need to introduce broad-ranging solutions that apply to all IoT devices, officials recommend that developing options to secure consumer smart devices would be a valuable first step.
29. This will involve developing options to secure devices available to everyday consumers. These may include personal and household devices, ranging from watches and other wearables to home routers, large appliances, and home entertainment systems.
30. Following international partners by starting with consumer smart devices would ensure we learn from their experience and ensure close alignment with partners' approaches. This would also allow us to test a New Zealand-appropriate approach before considering whether, or how best, to extend this to a broader range of IoT devices.
31. Other work being undertaken across the New Zealand system – including cyber resilience, protection of critical infrastructure and supply chain security – may also have impacts on industrial and commercial smart devices. Beginning with consumer smart devices will mean we can address the threats that face consumers now, and build on the other work being undertaken across the system in time.
32. Following the implementation of policies for consumer smart devices, officials would work on the identification of options to address critical/high risk devices/sectors in commercial/enterprise and industrial IoT, and eventually options to cover all IoT devices. Further advice on these further phases covering a broader range of devices will be provided at a later date.
33. There are factors that will need to be considered in the development of policy options. These include:
  - *Trade*: There may be impacts on pre-existing trade arrangements.
  - *Import/retail prices*: Lifting the security of IoT devices may increase costs to business and consumers.
  - *Innovation*: Any approach for securing IoT will need to ensure we are continuing to foster innovation in New Zealand.
  - *Implementation burdens*: The policy options will consider the potential burdens and costs of implementing and enforcing an approach.
  - *Regulatory impacts*: There will be appropriate consideration given to the associated costs and benefits of any policy option that includes regulatory change or creation.
  - *Time to roll out*: Timeframes for the proposed policy options will need to be considered to ensure we are developing up-to-date approaches.
  - *International alignment*: Aligning with our international partners will ensure that there is interoperability of standards to reduce implementation burdens for those responsible and optimise our efforts.

## Next Steps

---

34. Subject to your agreement, officials will begin the analysis and drafting of policy options for improving the security of consumer smart devices.



35. To inform the development of these options, officials will undertake informal targeted discussions with industry, to ensure any options factor in industry needs and concerns.
36. It will be essential that any policy options are consulted with industry and the public, in order to understand where the burden of cost/inconvenience might lie, what the social and economic implications could be, and to ensure broad buy-in to any potential options proposing regulatory change.
37. s9(2)(f)(iv) [REDACTED]

## Consultation

---

38. This briefing has been consulted with the following agencies:
  - CERT NZ
  - Department of Internal Affairs – Government Chief Digital Officer
  - Department of Internal Affairs – Government Chief Privacy Officer
  - Government Communications Security Bureau – Joint Director-Generals Office
  - Ministry of Business, Innovation and Employment – Competition and Consumer Affairs
  - Ministry of Business, Innovation and Employment – Digital, Communications and Transformation
  - Ministry of Business, Innovation and Employment – Radio Spectrum Management
  - Ministry of Foreign Affairs and Trade
  - Ministry of Justice
  - Standards NZ
  - Statistics NZ – Government Chief Data Steward