Australian Government

Department of Home Affairs

~~PROTECTED: Sensitive: Cabinet~~

TALKING POINTS

Subject	Launch of Australia’s 2020 Cyber Security Strategy		
Date	16 July 2020		
Type	Ministerial		
Media Officer:	s. 22(1)(a)(ii)	**Media Ph:**	02 6264 2244

ISSUE

Key messages and Q&As to support the launch of Australia’s 2020 Cyber Security Strategy.

TALKING POINTS UNCLASSIFIED

- Australia’s 2020 Cyber Security Strategy outlines Australia’s approach to keeping Australian families, vulnerable Australians, critical infrastructure providers and Australian business secure online.
- It is a strategy for all Australians and Australian businesses – from our telcos and energy providers to small business and the community – security is a whole-of-community effort, in which we all have a role to play.
- Cyber threats are growing in sophistication and scale - Cybercrime is a constant threat and we know that state-sponsored actors are actively targeting Australia.
- Cyber security enables consumer confidence which will grow the digital economy and support Australia’s recovery from the COVID-19 pandemic, as well as our future prosperity.
- Keeping Australians safe and secure online is key to protecting our economy, national security and sovereignty.
- The 2020 Strategy will invest $1.66 billion to build new cybersecurity and law enforcement capabilities, assist industry to protect themselves and raise the community’s understanding of how to be secure online.
  - This includes the landmark $1.35 billion Cyber Enhanced Situational Awareness and Response (CESAR) package and the Australian Government’s $156 million cyber security election commitments.
- This is the largest ever Australian Government investment in cyber security – reinforcing the Government’s ongoing commitment to keeping Australians safe and secure online.
- New capabilities for Australia’s cyber security agencies will help address sophisticated threats, particularly to the essential services all Australian’s rely on - everything from electricity and water, to healthcare and groceries.
- The Australian Government is developing an enhanced all-hazards security framework to bolster the nation’s resilience and ensure we can act in an emergency.
  - This framework will enhance the overall security of critical infrastructure, and the supply chains they rely on and supports industry calls for stronger leadership.

  - The framework includes a range of security obligations for critical infrastructure providers, including specific cyber security obligations and Government assistance to industry in response to immediate and serious cyber attacks on Australian systems

- Improving the security and resilience of critical infrastructure entities from a range of hazards– across all sectors– is crucial to protect our economy, security, and sovereignty.

- We will work with business to update legislation to ensure that critical infrastructure sectors deliver their essential services with security front of mind.

- We will give our law enforcement agencies increased ability to identify and disrupt cybercrime, including when criminals use the dark web and anonymising technologies to hide their activities.

- Businesses of all sizes will need to take steps to protect themselves and their customers.

  - Government will assist with hands on support, advice and a clear regulatory environment.

- The community will always have a role to play in cyber security.

  - Government will provide increased support to the community through an expanded 24/7 cyber hotline and support services for victims of cybercrime.

- Our work does not stop here. An expanded Industry Advisory Committee will be formed to guide implementation of the Strategy and continue to address cyber security threats in the longer-term.

- Australia’s landmark Cyber Security Strategy delivered in 2016 has driven cyber security innovation and economic prosperity, and positioned Australia as a leader in cyber security.

- The 2020 Cyber Security Strategy builds on the strong foundations established by its predecessor, investing in:

  - Protection of the critical infrastructure that all Australians rely on, including cyber security obligations on owners and operators.
  - New ways to investigate and shut down cyber crime.
  - Stronger defences for Government networks and data
  - Greater collaboration to build Australia’s cyber skills pipeline.
  - Increased situational awareness and improved threat information sharing.
  - Stronger partnerships with business through the Joint Cyber Security Centre Program
  - Tailored advice and support for small and medium enterprises to increase their cyber resilience.
  - Clear guidance for businesses and consumers about securing Internet of Things devices.
  - 24/7 enhanced support for victims of cyber crime.
  - Improved community awareness of cyber security threats.

- The Strategy is based on extensive consultation and expert advice.

  - More than 1,400 people attended a consultation event and 215 submissions were received.
  - The Strategy has been informed by extensive consultation and expert advice from an Industry Advisory Panel, chaired by Telstra CEO Andy Penn.

What are the threats?

- Australia's cyber security posture has advanced markedly, however, so too have the online threats from malicious actors and cyber criminals.
- Malicious cyber activity against Australia's national and economic interests is evolving in scale, sophistication and impact.
- State based actors, cyber criminals and other malicious actor groups are threats to our economy, our strategic interests and our way of life and are exploiting Australians for financial gain.
- We cannot be complacent. An incident involving Australia's critical infrastructure has the potential to cause significant consequences across our economy, security and sovereignty.
  - Disruption to one element of these services could have a domino effect to others, significantly affecting our way of life.
  - Owners and operators of critical infrastructure across a range of sectors are facing evolving threats, including increasing cyber attacks, in the midst of a global health pandemic and tough economic landscape.
- AustCyber estimates a significant cyber attack impacting Australia for four weeks could cost the economy $30 billion, or around 1.5% of GDP, and an estimated loss of 163,000 jobs.
- Criminals are leveraging the internet and the dark web to buy and sell stolen identities, illicit commodities, trade child exploitation material and buy accesses to Australian computers and networks to facilitate further crime.
  - New encryption and anonymising technologies allow criminals and others to hide their identity and activity from law enforcement agencies.
- Health service providers, the finance sector, legal, accounting and management services, education and personal services are the top five industry sectors targeted by malicious or criminal attacks and cyber incidents.
  - Between July and December 2019, 94 per cent of data breaches in the finance sector were attributed to cyber incidents.

Has there been a significant rise in cyber threats during COVID-19?

- The COVID-19 pandemic has highlighted how much we live and work online – trusting the internet for healthcare, business, education, entertainment, social connection and online shopping.
- Malicious actors are taking advantage of the COVID-19 pandemic to target Australian families and businesses.
  - Cyber criminals are tailoring their attacks to exploit COVID-19 related messaging and targeting essential services with ransomware.

- Cybercriminals are adapting their online criminal methods to take advantage of the pandemic, and state-based actors actively targeting health sector organisations and medical research facilities.
    - On 8 May 2020 the ACSC issued Advisory 2020-009: Alerting the public to Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services on 8 May 2020.
    - On 17 July, Australia declared its support for the Joint Cyber Security Advisory by the US, UK and Canada, which detailed malicious cyber activity by Russian actors targeting organisations involved in COVID-19 vaccine development.
- Businesses operating in key supply chain networks transporting groceries and medical supplies have also been targeted.

Who is the strategy for?

- Cyber security is a whole of community task. Everyone has a role to play in creating a more cyber secure Australia – Government, businesses and the community.
- An effective Cyber Security Strategy can only be achieved through strong partnerships that drive cyber resilience across the economy.
- Government's focus will be on critical threats and the most sophisticated actors, while ensuring a baseline level of cyber resilience across the economy.
- Businesses will take responsibility for addressing more common cyber security threats, in the same way that businesses are responsible for the safety and quality of their products.
    - The government will support business by providing trusted, practical advice to small businesses and by working hand in glove with critical infrastructure owners to identify and resolve immediate vulnerabilities.
- The community will always have a role to play in cyber security.
    - Even with the best efforts of Government and businesses, Australians will need to know how to safeguard themselves against cyber security threats.
    - The best thing you can do to be secure is to stay informed. You can start by visiting cyber.gov.au for tips and up to date advice.

How will the strategy directly help families and individuals in the community?

- Not all cyber security risks can be addressed by governments and business.
- To support improved cyber security in the community, the Australian Government will:
    - expand efforts to raise awareness of cyber security threats and drive uptake of safe and secure online behaviours across the community
    - expand our 24/7 cyber security advice hotline for families and older Australians.
    - increase funding for victim support

  - introduce a voluntary Internet of Things Code of Practice to inform manufacturers about best practices for securing devices and help consumers make informed purchasing decisions.

How will the strategy directly help small businesses?

- Businesses of all sizes will need to take steps to protect themselves and their customers.
- Government will assist with support, advice and a clear regulatory environment including:
  - expanding efforts to raise awareness of cyber security threats and drive uptake of safe online behaviours across the community
  - an $8.3 million Cyber Security Connect and Protect program will equip trusted organisations to raise the cyber security of SMEs in their local area
  - the placement of outreach officers in Joint Cyber Security Centres to support small and medium businesses
  - supporting the roll out of threat blocking technology to prevent known virus and scams from reaching Australian consumers and businesses
  - toolkits for small and medium businesses to raise cyber security awareness among their staff
  - offering stronger support through a dedicated cyber security training program
  - expanding our 24/7 cyber security advice hotline for small and medium enterprises, families and older Australians
  - encouraging more secure devices for all consumers and businesses through the introduction of a voluntary Internet of Things Code of Practice to inform manufacturers about best practices for securing devices.

How will the strategy help protect those businesses delivering our essential services?

- Improving the security and resilience of critical infrastructure entities – across various sectors– is crucial to protect our economy, security, and sovereignty.
- The Australian Government has agreed to an enhanced security framework to bolster the nation's resilience and ensure we can act in an emergency.
- The proposed framework includes:
  - a security obligation for critical infrastructure entities, supported by sector-specific requirements
    - The security obligation will require owners and operators of critical infrastructure in Australia protect their assets and operations from all hazards, including cyber.
  - enhanced cyber security obligations for those entities most important to the nation, centring around a strengthened relationship with Government.

  - Government assistance to industry in response to immediate and serious cyber incidents impacting Australia's critical systems.

- The Government recognises that Australia is more resilient and secure when we work together.
- To respond to the evolving threat environment, the Government will build on its existing industry partnerships and work with critical infrastructure owners and operators) to protect the essential services all Australians rely on.
- The reforms are designed to ensure that those entities who take security seriously are not at a commercial disadvantage.
- The Government has proposed a range of measures to enhance its partnership with critical infrastructure entities including:
  - Co-designing best practice guidance, recognising that across critical infrastructure sectors, one size does not fit all
  - Delivering workshops, conducting joint cyber exercises and vulnerability assessments
  - Delivering near-real time national threat information sharing
  - Empowering critical infrastructure entities to appropriately protect themselves when faced with a serious threat.
- Critical infrastructure entities will benefit from:
  - Strengthened security of networks and systems that underpin their business
  - Access to cyber threat information shared by Government
  - Government's assistance to protect their assets and mitigate damage from cyber attacks in an emergency.

Who will the critical infrastructure reforms apply to?

- Government will partner with critical infrastructure entities – across various sectors and regardless of ownership – to ensure the reforms are targeted at the networks, systems and assets most critical to Australia's economy, security and sovereignty.
- We will work with industry, academia, and state and territory governments and industry-specific regulators to determine which sectors and entities the reforms will apply to.
- We recognise that one size does not fit all.
  - The initial focus of consultation will be to design the high level legislative framework principles, obligations and actions.
  - We recognise that some entities, particularly those with long-standing and close relationships with national security agencies, already have robust security procedures in place.
- We will then work closely with industry, states and territories industry-specific regulators, and our international partners to co-design sector-specific obligations.

What sectors are included in the critical infrastructure reforms?

The reforms expand the application of the *Security of Critical Infrastructure Act 2018* to a broad range of sectors including:

- banking and finance
- food and grocery
- health
- transport
- energy
- water
- communications
- space
- data and the cloud
- higher education, research and innovation
- defence industry

Will the critical infrastructure reforms create regulatory burdens for businesses?

- We will work with industry, academia, and state and territory governments to develop these reforms.
- By working together, we aim to minimise costs and duplication of existing regulatory and policy requirements for industry (where possible) and ensure that entities who take security seriously are not at a commercial disadvantage.
- All businesses can expect to benefit from an uplift of security and resilience across critical infrastructure sectors, ensuring continuity and security in the networks, systems and services they rely on.

Will the critical infrastructure reforms impact foreign investment?

- The framework will create an even playing field:
  - applying to owners and operators of critical infrastructure regardless of ownership
  - ensuring critical infrastructure entities who take security seriously are not at a commercial disadvantage.
- Australia's investment policy settings continue to be open and, transparent.

Why does business need Government's assistance

- The security and resilience of critical infrastructure is crucial to protecting our economy, security, sovereignty and the well-being of all Australians.

- Consultation with Australian business, the community and academia has revealed an increasing expectation for Government to play a stronger role in supporting business to manage their security responsibilities through clear regulations and standards that apply across critical assets.
- Business has also called for stronger leadership on critical infrastructure security and resilience.
- If there was a significant incident affecting the one or multiple business sectors, the public and business would expect leadership from the Government.
- For these reasons, and only in limited emergency circumstances, where there is an immediate and serious cyber threat, the Government will have the power to provide advice and assistance on mitigating damage and restoring services, and to defend and protect a network or system in the national interest..
- The Government will work with business to develop these reforms to protect Australia's most significant systems from the most significant threats.

If asked: Will Government's assistance to industry to protect critical infrastructure include financial assistance?

- No. The Government will provide direct assistance through information sharing and advice.
- While critical infrastructure entities are primarily responsible for their own security, there are some threats too sophisticated or disruptive to be handled alone.

s. 7(2A)

[redacted]

If asked: How will Government know when an emergency is happening? Will they be monitoring the systems designated as systems of national significance?

s. 7(2A)

[redacted]

- These reforms will ensure that our critical infrastructure owners and operators deliver their essential services within a robust security framework to manage and mitigate threats to those services.
- They will also include the ability for Government to assist entities in emergencies.
- This is something industry has asked for and we are consulting with industry in order to design effective reforms.

If asked: Does this effectively mean that ASD will be spying on Australians?

- No. The Australian Government is working closely with industry to respond to new and increasing threats.
  - This package is about securing and protecting Australia's critical infrastructure – the essential services that all Australians rely on every day.

What impact will the Cyber Security Strategy have on Australian businesses?

- The purpose of developing the new Strategy is to protect Australia's prosperity from the growing cyber threat environment. This will be good for business and our society as a whole.

What is government doing to better secure Commonwealth systems?

- The 2020 Cyber Security Strategy will continue and sharpen our focus on protecting government networks from the growing threat environment.
- This may include centralising IT security systems across the Commonwealth agencies into various hubs.
  - This will strengthen Commonwealth agencies' cyber security postures by reducing the number of entry points for malicious actors and decommissioning older systems.
  - Where possible, the Australian Government will also seek to automate cyber security functions and create efficiencies such as through standard cyber security contractual clauses.

Where can people get more information?

- The 2020 Cyber Security Strategy is available at www.homeaffairs.gov.au/cybersecurity.
- The Australian Government has developed and published extensive material for individuals on how to stay secure and safe online.
  - For cyber security advice and to report an incident visit Cyber.gov.au.
  - For online safety advice and to report an incident visit esafety.gov.au.
  - For online scam advice and to report a scam visit scamwatch.gov.au.

If asked: Is the timing of the new Cyber Security Strategy related to the PM's announcement of state-based cyber activity targeting Australia?

- No, the Government is on the front foot when it comes to cyber security.
- The methods used by malicious cyber actors are continually evolving and Australia is constantly exposed to cyber threats. That's why we must constantly adapt, improve and evolve.
- This new Cyber Security Strategy takes a whole of economy approach and ensures Australia keeps pace with the fast changing cyber environment.
- The Strategy has been informed by extensive consultation and expert advice from an Industry Advisory Panel, chaired by Telstra CEO Andy Penn.
  - More than 1,400 people attended a consultation event and 215 submissions were received.

If asked: Do we need a dedicated Minister for Cyber Security?

- The Minister for Home Affairs has responsibility for national cyber security policy.
- Cyber security and online safety are a shared responsibility, and Government agencies contribute to this collective effort alongside business, the community, and the states and territories.
- Like all complex policy areas there are mechanisms across government to ensure our efforts remain coordinated.

If asked: Has the Government left the Opposition out of the cyber security conversation?

- This Strategy is for all Australians and follows extensive consultation and expert advice.
- We will continue to work in close partnership with all levels of government, business and the community to create a more cyber secure Australia.
- Keeping Australians safe and protecting Australia's economy, national security and sovereignty are priorities for the Government.

If asked: Will the proposed powers for law enforcement give them more access to people's encrypted data and further degrade the privacy of Australians?

- The Cyber Security Strategy is about protecting Australian government, businesses, families and individuals.
- The Government is supportive of encryption and the communications industry's efforts to provide a secure online environment for users.
- Transnational Serious and Organised Crime groups and cyber criminals are agile and have no regard for geographical or traditional boundaries – they respond quickly to significant

international and national disasters, like the COVID-19 global pandemic and the 2019-20 bushfires.

- The increasingly widespread use of the dark web, and other technologies that allow illegitimate users to remain anonymous, to enable serious crime and terrorism is inhibiting agencies' ability to protect our community – including protecting children from sexual abuse.
  - Our laws must change to close the investigative gaps that make it almost impossible in the early steps to identify the serious criminals operating online.
- The Government can and will act – to ensure agencies have the powers and capabilities they need to identify and disrupt these increasing, and very real, threats.
- The community can be assured that any powers to help our agencies remain effective in protecting our community will include strong oversight and review mechanisms and be balanced against the economic and cultural benefits that online connectivity brings and the privacy of legitimate users.

If asked: What did the Government achieve through the 2016 Cyber Security Strategy?

- The 2016 Cyber Security Strategy provided a clear national focus on cyber security. Under the 2016 Strategy, the Government has:
  - launched Joint Cyber Security Centres in Sydney, Melbourne, Adelaide, Brisbane and Perth to work with business and government to strengthen partnerships and protect critical infrastructure against malicious cyber activity
  - opened the Australian Cyber Security Centre (ACSC), bringing together the Government's cyber expertise into one dedicated facility and strengthening our ability to meet current and emerging threats
  - helped Australia's world class cyber security industry capitalise on new commercial opportunities through initiatives such as AustCyber (the Australian Cyber Security Growth Network)
  - strengthened Australia's cyber security workforce through the establishment of Academic Centres of Cyber Security Excellence at Edith Cowan University and the University of Melbourne
  - appointed Australia's first Cyber Affairs Ambassador and published Australia's International Cyber Engagement Strategy
  - partnered with international counterparts to call out state-sponsored malicious cyber activity and support international norms that ensure a free and open internet for all.

If asked: Why haven't all the measures announced under the 2016 Cyber Security Strategy's action plan been delivered yet?

- The 2016 Cyber Security Strategy is complete. A number of actions will continue into the future, such as consulting business on cyber security matters and assisting government departments to raise their cyber security posture.

- Implementing the 2016 Cyber Security Strategy has strengthened Australia's cyber security foundations, stimulated private sector investment in the domestic cyber security industry and positioned Australia as a regional cyber security leader.

What is the Cyber Enhanced Situational Awareness and Response (CESAR) package?

- The Cyber Enhanced Situational Awareness and Response (CESAR) package will invest $1.35 billion over the next decade to combat malicious cyber activity.

- The CESAR package has been designed to boost protection and cyber resilience for all Australians, from individuals and small businesses through to the providers of critical services and government.

- This package is one part of a broader $15 billion investment in cyber and information warfare capabilities that forms part of the Defence Force Structure Plan.

- The package includes $470 million to expand the Government's cyber security workforce creating 500 new jobs within the Australian Signals Directorate.

s. 7(2A)

[redacted]

- $200 million will be spent on bolstering our understanding of malicious cyber activity, including expanding intelligence capabilities to improve situational awareness and ensure Australia remains at the forefront of technological advancements in cyber security.

If asked: Why was the Strategy late?

- Government committed to update the Strategy in 2020. The announcement today has fulfilled that commitment.

If asked: Is the increase in Cyber security spending in response to China?

- The Cyber Security Strategy is strategy for all Australians and Australian businesses – from our critical infrastructure providers to small business and the community.

- It is not in response to a single threat, to a particular criminal group or any one nation.

- Malicious cyber activity is increasing in frequency, scale, sophistication and impact.

- Regrettably, this is part of the new world we live in.
- This is why we are making the single largest investment in our nation's cyber security.

If asked: Why does the Government only attribute some malicious cyber activity?

- The Government will only make an attribution when it is clear and in our national interest to do so.
- We assess each incident, and calibrate our responses, on a case-by-case basis
- Public attribution is just one of many responses that Australia has in its toolkit.
- And not all of Australia's responses to cyber incidents will be public.
- Regardless of the context, Australia's responses will always be proportionate, comply with domestic law, and be consistent with international law and the norms of responsible state behaviour that we expect all countries to follow
    - This puts Australia at the forefront of efforts to promote a peaceful and stable online environment.

If asked: What is the Government doing to counter COVID-19-related malicious cyber activity?

- The Government is working hard to protect Australians from COVID-19 related cyber threats.
    - We know some cyber offenders have tailored their attacks to exploit COVID-19 related messaging.
    - We also know malicious cyber actors may target intellectual property relating to vaccine development, treatments, research and responses to the outbreak.
- During the COVID-19 crisis, the ACSC has produced multiple COVID-19-related threat advisories and tailored cyber security advice on how Australians can best protect themselves from cyber-attacks.
- The Australian Cyber Security Centre (ACSC), assisted by law enforcement and business partners, is working to disrupt and prevent malicious cyber activity exploiting the COVID-19 pandemic.
    - The ACSC is also working with hospitals and health service providers to reduce their risk of cyber compromise during this challenging period.
- All citizens, businesses and institutions should be extra vigilant regarding COVID-19 related communications.
- Internationally, the Government is collaborating with international partners, to monitor and respond to this malicious activity, including sharing intelligence, lessons learned and identifying disruption opportunities

If asked: What is the Government doing internationally on Cyber Security?

- Internationally, Australia is committed to working with our allies and partners when it comes to managing cyber security threats, including developing capacity to address cyber threats and sharing best practices
    - Australia is engaged in negotiations at the UN to deepen understanding of, and promote adherence to, the agreed rules of the road for countries in cyberspace
    - in September 2019, Australia, the US and the UK launched the Joint Statement on Advancing Responsible State Behaviour in Cyberspace
        - this Statement makes clear the importance of holding accountable those countries that engage in malicious cyber activity
        - to date, 28 countries have signed up to the Statement.

If asked: How does the Strategy match up against the Industry Advisory Panel's report?

- The Strategy aligns with the recommendations of the Industry Advisory panel.

If asked: Who will be included in the Industry Advisory Committee?

- Government will provide further information on the makeup and scope of the committee at a later time.

CLEARANCE

Drafted by	**Title**	**Time/Date drafted**
s. 22(1)(a)(ii)	Public Affairs Officer	16 July 2020
Consultation	ACIC, Treasury, ONI, DIRDTC, AFP, ASIO, AGD, Defence, ASD, DISER, DFAT, Services Australia, PM&C, DESE	

Cleared by	**Title**	**Time/Date cleared**

s. 22(1)(a)(ii)	A/g Assistant Secretary, Cyber Policy and Strategy Branch – Cyber Security and Intelligence Division	6:45pm 3 August 2020
Andrew Kiley	Assistant Secretary, Assurance, Risk and Engagement Branch, Critical Infrastructure Security Division	8:36pm 3 August 2020
Andrew Warnes	Assistant Secretary, National Security Policy Branch, Law Enforcement Policy Division	10:48am 3 August 2020
s. 22(1)(a)(ii)	Director, National Security and Crisis Communication – Media and Communication Branch	10:05pm 3 August 2020

MO noted	**Sent to MO**	**Noted by MO**
Full Name	Time DD MM 2020	Time DD MM 2020

THE HON SCOTT MORRISON MP
PRIME MINISTER

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

JOINT MEDIA RELEASE

XX August 2020

LAUNCH OF AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

The Australian Government has today launched Australia's 2020 Cyber Security Strategy to keep all Australians secure online and protect the essential services we all rely on.

Prime Minister Scott Morrison said effective cyber security was central to protecting the community and Australia's economy, national security and sovereignty.

"Cyber threats targeting Australians are growing in sophistication and scale," the Prime Minister said.

"Cyber crime is a constant problem. We are facing increasing threats to essential services, businesses and all levels of government and we know that state-sponsored actors are actively targeting Australia,"

"Cyber security encourages and facilitates the innovation that will help us grow the digital economy to support Australia's recovery from the COVID-19 pandemic, as well as our future prosperity.

"This is a strategy for all Australians and Australian businesses – from our telcos and energy providers to small business and the community – security is a whole-of-community effort, in which we all have a role to play.

"The 2020 Cyber Security Strategy represents the single greatest Australian Government financial commitment to cyber security.

Including the landmark $1.35 billion Cyber enhanced Situational Awareness and Response package and the Australian Government's $156 million cyber resilience and workforce package, the 2020 Cyber Security Strategy brings together $1.66 billion to build new cybersecurity and law enforcement capabilities, assist industry to protect themselves and raise the community's understanding of how to stay safe online."

Minister for Home Affairs Peter Dutton said the Strategy would significantly boost capabilities to better deter, prevent and respond to the most significant threats, setting out a plan for Government, business and the community to work together to protect Australians online.

“Agencies will be equipped to help address sophisticated threats, particularly to the essential services all Australian’s rely on - everything from electricity and water, to healthcare and groceries.

“We are introducing a security framework to bolster the nation’s resilience and ensure we can act in an emergency. The framework includes security obligations for critical infrastructure providers and Government assistance to industry in response to immediate and serious cyber attacks on Australian systems.

“Improving the security and resilience of critical infrastructure entities is crucial to protect our economy, security, and sovereignty. We will work with owners and operators of critical infrastructure to update legislation to ensure that critical infrastructure sectors deliver their essential services with security front of mind.

“The Strategy outlines steps businesses of all sizes can take to protect themselves and their customers, and the Government will be there to help with support, advice and a clear regulatory environment.

“Transnational Serious and Organised Crime groups and cyber criminals are agile and have no regard for geographical or traditional boundaries. We will give our law enforcement agencies increased ability to identify and disrupt cybercrime, including when criminals use the dark web and anonymising technologies to hide their activities, boosting their ability to protect our community – including protecting children from sexual abuse.

“All of us have a role to play in keeping our own online environment safe but government will be there to help through an expanded 24/7 cyber hotline and professional support services for victims of cyber crime.”

The 2020 Cyber Security Strategy builds on the strong foundations established by its predecessor, investing in:

- protection of the critical infrastructure that all Australians rely on
- new ways to investigate and shut down cyber crime
- stronger defences for Government networks and data
- greater collaboration to build Australia’s cyber skills pipeline
- increased situational awareness and improved threat information sharing
- stronger partnerships with industry through the Joint Cyber Security Centre Program
- tailored advice and support for small and medium enterprises to increase their cyber resilience

- clear guidance for businesses and consumers about securing Internet of Things devices
- 24/7 support for victims of cyber crime
- improved community awareness of cyber security threats.

The Strategy has been informed by extensive consultation and expert advice from an Industry Advisory Panel, chaired by Telstra CEO Andy Penn.

Australia's 2020 Cyber Security Strategy is available at www.homeaffairs.gov.au/cybersecurity.

Prime Minister's Office – XXXX
Minister Dutton's Office – 02 6277 7860
Minister Reynolds' Office – XXXX

Cleared by	**Title**	**Time/Date cleared**
s. 22(1)(a)(ii)	A/g Assistant Secretary, Cyber Policy and Strategy Branch	6:45pm 3 August 2020
Andrew Kiley	Assistant Secretary, Assurance, Risk and Engagement Branch	8:36pm 3 August 2020
Andrew Warnes	Assistant Secretary, National Security Policy Branch	10:48am 3 August 2020
s. 22(1)(a)(ii)	Director National Security and Crisis Communication	10:31pm 3 August 2020

Australian Government

Department of Home Affairs

TALKING POINTS

Subject	Dark Web status update - Minister		
Date	4 August 2020		
Type	Ministerial		
Media Officer:	s. 22(1)(a)(ii) [redacted]	**Media Ph:** 02 6264 2244	

ISSUE

The Minister would like to make a public statement about where the Government is at in response to the challenges laid out by the AFP, AUSTRAC and the ACIC at the National Press Club about the dark web and other anonymising technologies.

TALKING POINTS UNCLASSIFIED

- The Government will not stand idly by, in the face of increasing threats to the safety and security of Australians – including children and other vulnerable members of our community.
- The increasingly widespread use of the dark web and other technologies that allow illegitimate users to remain anonymous to enable serious crime and terrorism, is inhibiting agencies' ability to protect our community – including protecting children from sexual abuse.
    - o Criminals are leveraging the internet and dark web to buy and sell stolen identities, illicit commodities, trade child exploitation material and facilitate other serious crimes.
- While advances in technology have helped hide criminals, they have made things much harder for our enforcement agencies.
- Our laws must catch up with technology if our agencies are to continue to do the job we expect of them – to keep Australians safe.
- To meet this challenge we are developing legislative powers that will substantially boost the capacity of the Australian Federal Police and the Australian Criminal Intelligence Commission to fight cyber-enabled serious crime.
- The agencies know these nefarious activities are taking place but on the dark web, or under the cloak of other anonymising technologies, collecting even basic intelligence such as identities is extremely difficult under existing laws,
- We need to enable the AFP and the ACIC to identify targets of interest in relation to the most serious crime types including terrorism, child abuse offences and drug and firearms trafficking.

  - Right now, the AFP and the ACIC can only collect communications in relation to an investigation of a particular person or device, connected with a specific offence, under warrant.
  - The characteristics of the dark web and anonymising technologies, such as encryption, make identifying suspects extremely difficult.
- It will be easier for the AFP and ACIC to identify serious criminals if they have enhanced access to criminal communication networks that enable serious offending, .
  - We plan to introduce a new power that would give the AFP and ACIC the ability to target criminal networks operating online, including on the dark web, by permitting access to the computers used to facilitate serious criminal activity.
  - This would enable that vital first investigative step of identifying perpetrators and the scope of their offending, amidst the mass of information on the dark web.
  - Information collected under this power will inform applications for more targeted investigatory powers, such as interception and computer access warrants.
- The powers will be limited to uncover only serious criminal acitivity, with corresponding thresholds and robust oversight.
- The Government also recognises that the disruption of some online activities, such as the sharing of child abuse images, should not have to wait for the completion of what can be a lengthy investigation.
  - In carrying out an investigation, agencies may become aware of an online database of child abuse images, for example
  - Allowing agencies to disrupt such activity, for example by deleting the child abuse images to prevent their proliferation on the internet, would help protect the victims and potentially prevent further crimes.
- The community can be assured that any powers to help our agencies remain effective in protecting our community will include strong oversight and review mechanisms and be balanced against the economic and cultural benefits that online connectivity brings and the privacy of legitimate users.
- The government will continue to ensure agencies have the powers and capabilities they need to identify and disrupt threats to the safety of Australians – particularly children, the most vulnerable members of our community

If asked: Will the proposed powers for law enforcement give them more access to people's encrypted data and further degrade the privacy of Australians?

- The Cyber Security Strategy is about protecting Australian government, businesses, families and individuals.
- The Government is supportive of encryption and the communications industry's efforts to provide a secure online environment for users.

- Transnational Serious and Organised Crime groups and cyber criminals are agile and have no regard for geographical or traditional boundaries – they respond quickly to significant international and national disasters, like the COVID-19 global pandemic and the 2019-20 bushfires.

- The increasingly widespread use of the dark web, and other technologies that allow illegitimate users to remain anonymous, to enable serious crime and terrorism is inhibiting agencies' ability to protect our community – including protecting children from sexual abuse.
  - Our laws must change to close the investigative and intelligence collection gaps that make it almost impossible to identify the serious criminals operating online.

- The Government can and will act – to ensure agencies have the powers and capabilities they need to identify and disrupt these increasing, and very real, threats.

- The community can be assured that any powers to help our agencies remain effective in protecting our community will include strong oversight and review mechanisms and be balanced against the economic and cultural benefits that online connectivity brings and the privacy of legitimate users.

How do these new technical powersintersect with the ASD/ Will some of these new technical powersinvolve diverting or duplicating activities currently only undertaken by the Australian Signals Directorate?

- The new powers being proposed are for the AFP and the ACIC.
- They do not change or expand ASD's powers.
- Consistent with its functions under the ISA, ASD is empowered to provide AFP and ACIC with technical expertise and assistance.
- Along with its foreign intelligence mission, the Australian Signals Directorate's existing powers and functions include working with other Australian Government agencies and approved international partners, and providing specialised advice and assistance to Australian authorities that allows them to meet cyber threats, counter cybercrime and minimise harm to Australians.

How will the disruption power be used? What sort of authorisation would be required?

- The authorisation for use of these powers will be developed using the basis of the requirements for existing law enforcement powers.
- As with all aspects of law enforcement powers and operations, there will be strict oversight and review mechanisms in place.
- Robust authorisation and oversight frameworks will be a hallmark of this legislation.
- The Government will continue to ensure agencies have the powers and capabilities they need to identify and disrupt threats to the safety of Australians – particularly children, the most vulnerable members of our community.

What's the timeframe for implementing these reforms?

- The Government will continue to finalise the legislation to underpin these new powers.
- The Government will continue to ensure agencies have the powers and capabilities they need to identify and disrupt threats to the safety of Australians – particularly children, the most vulnerable members of our community.

CLEARANCE

Drafted by	**Title**	**Time/Date drafted**
s. 22(1)(a)(ii)	Public Affairs Officer	4 August 2020
Consultation	ACIC, AFP, ASD	

Cleared by	**Title**	**Time/Date cleared**
Andrew Warnes	Assistant Secretary, National Security Policy Branch, Law Enforcement Policy Division	12:01pm 5 August 2020
s. 22(1)(a)(ii)	Director, National Security and Crisis Communication – Media and Communication Branch	12:08pm 5 August 2020

MO noted	**Sent to MO**	**Noted by MO**
Full Name	Time DD MM 2020	Time DD MM 2020

Environment

Australia is facing increasing cyber security threats to essential services, businesses and all levels of government. Malicious cyber activity against Australia's national and economic interests is evolving in scale, sophistication and impact. In June, based on advice from our cyber experts, I advised that Australian organisations were being targeted by a sophisticated state-based actor.

The COVID-19 pandemic has highlighted how much we live and work online – trusting the internet for healthcare, business, education, entertainment, social connection and online shopping.

Keeping Australians safe and secure online is key to protecting our economy, national security and sovereignty. Cyber threats targeting Australians are growing in sophistication and scale. Cybercrime is a constant threat

Cyber security encourages and facilitates innovation that will grow the digital economy to support Australia's recovery from the COVID-19 pandemic, as well as our future prosperity.

Cyber Strategy

Today we are releasing Australia's 2020 Cyber Security Strategy. The Strategy, backed by Australia's largest ever investment in Cyber Security of $1.66 billion is a Strategy for All Australians and Australian businesses – from our big telcos and energy providers to small business and the community, we all have a role to play.

This $1.66 billion investment includes the landmark $1.35 billion Cyber Enhanced Situational Awareness and Response (CESAR) package we announced in June and the Australian Government's $156 million cyber resilience and workforce package.

More than that, the Strategy provides advice and assistance to keep Australian families, vulnerable Australians, critical infrastructure providers and Australian business safe and secure online.

Ultimately, all the measures in the strategy are designed to protect us and our way of life - whether they are aimed at the businesses who keep our essential services running, the businesses that make our lives easier by allowing us to, shop, learn, and entertain ourselves online, or advice for us all as we live, work and connect with each other.

SOCI/SONS

At the most sophisticated but also the most basic level, we need to ensure the continuation of the services we all depend on - everything from electricity and water, to healthcare and groceries – in the face of sophisticated threats.

An incident involving Australia's critical infrastructure has the potential to cause significant consequences. Disruption to one element of these services could have a domino effect to others, significantly affecting our way of life.

Owners and operators of critical infrastructure across a range of sectors are facing evolving threats, including increasing cyber attacks, in the midst of a global health pandemic and tough economic landscape.

AustCyber estimates a significant cyber attack impacting Australia for four weeks could cost the economy $30 billion, or around 1.5% of GDP, and an estimated loss of 163,000 jobs.

Improving the security and resilience of critical infrastructure entities – across the various sectors - banking and finance, food and grocery, health, transport, energy, water, communications, space, data and the cloud, higher education, research and innovation, and defence industry - is crucial to protect our economy, security, and sovereignty.

With this in mind, the Australian Government will introduce an enhanced security framework to bolster the nation's resilience and ensure we can act in an emergency.

Key to the proposed framework will be a security obligation for critical infrastructure entities, supported by sector-specific requirements. The security obligation will require owners and operators of critical infrastructure in Australia protect their assets and operations from all hazards. There will be enhanced cyber security obligations for those entities most important to the nation.

The cyber security obligations centre around a strengthened relationship with Government through the provision of situational awareness on Government request, participation in preparatory activities (which could include proactive testing for vulnerabilities), co-development of a playbook detailing response plans for a range of scenarios.

While critical infrastructure entities are responsible for their own security, there are some threats too sophisticated or disruptive to be handled alone. To that end, the framework will include the ability for government to provide direct assistance to those networks and businesses most critical to the nation, in response to immediate and serious cyber attacks on Australian networks.

The Australian Government must be ready to act in the national interest when its unique capabilities are needed, especially in emergency situations. In consultation with critical infrastructure owners and operators, the Australian Government will develop new powers proportionate to the consequences of a sophisticated and catastrophic cyber attack, accompanied by appropriate safeguards and oversight mechanisms. These powers, the first in the world, will ensure the Australian Government can actively defend networks and help the private sector recover in the event of a cyber attack, including through defensive and offensive cyber capabilities.

Australians expect the Government to act in an emergency to support the national interest and this is what these arrangements will allow us to do. In limited emergency circumstances, where there is an immediate and serious cyber threat, the Government will have the power to actively defend and protect a network or system, and provide advice and assistance on mitigating damage and restoring services. The Government will closely partner with industry to implement near-real time threat information sharing to strengthen Australia's situational awareness of critical networks and protect critical infrastructure.

Government will work with critical infrastructure entities – across various sectors and regardless of ownership – to ensure the reforms are targeted at the networks, systems and assets most critical to Australia's economy, security and sovereignty.

We will work with industry, academia, state and territory governments and industry-specific regulators to develop the framework. We recognise that one size does not fit all and that some entities, particularly those with long-standing and close relationships with national security agencies, already have robust security procedures in place. The reforms are designed to ensure that those entities who take security seriously are not at a commercial disadvantage

SMES

But the cyber security strategy isn't just about protecting our critical infrastructure. Small and medium businesses are the backbone of our economy. There are around two million of them in Australia, and while they will need to take steps to protect themselves and their customers, we recognise many don't have the resources to employ in-house cyber expertise.

Government will assist with support, advice and a clear regulatory environment. An $8.3 million Cyber Security Connect and Protect program will equip trusted organisations to raise the cyber security of small and medium businesses in their local area and we will place outreach officers in Joint Cyber Security Centres to support small and medium businesses

We will support the roll out of threat blocking technology to prevent known virus and scams from reaching Australian consumers and businesses, develop toolkits for small and medium businesses to raise cyber security awareness among their staff. and offer stronger support through a dedicated cyber security training program.

We will also introduce a voluntary Internet of Things Code of Practice to inform manufacturers (and those who sell them) about best practices for securing devices.

Small and medium businesses will also benefit from an expansion of the ACSC's 24/7 cyber security advice hotline for small and medium enterprises, families and older Australians efforts to raise awareness of cyber security threats and drive uptake of safe online behaviours across the community.

Community

While the community will certainly benefit from the protection of our national systems and better security from businesses trading online, we are also putting in place other measures that will directly benefit families and our most vulnerable.

Cyber threats targeting Australians are growing in sophistication and scale - Cybercrime is a constant threat The increasingly widespread use of the dark web, and other technologies that allow illegitimate users to remain anonymous, to enable serious crime and terrorism is inhibiting agencies' ability to protect our community – including protecting children from sexual abuse.

We will give our law enforcement agencies increased ability to identify and disrupt cybercrime, including when criminals use the dark web and anonymising technologies to hide their activities. The Australian Government will also invest in a cyber crime 'capability uplift fund' to provide practical support to state and territory police, and bolster the Australian Federal Police's ability to investigate and prosecute cyber criminals.

Not all cyber security risks can be addressed by governments and business so we are providing some practical help to support improved cyber security in the community.

The Government will expand efforts to raise awareness of cyber security threats and drive uptake of safe and secure online behaviours across the community, and expand our 24/7 cyber security advice hotline for families and older Australians.

The Internet of Things Code of Practice will not only provide advice to manufacturers but will also help consumers make informed purchasing decisions.

And for those that fall victim to cyber criminals, we are increasing funding for victim support organisation IDCARE.

Government

And the Government's role isn't just about supporting business and the community with cyber security. We also have work to do – leading by example and continuing to ensure Government systems meet robust cyber security standards in order to protect the data and information of all Australians. It is a responsibility of all Australian Governments to protect the data we hold and to protect our systems from attack.

CESAR Package

The Cyber Security Strategy includes and is backed by the Cyber Enhanced Situational Awareness and Response (CESAR) package with $1.35 billion over the next decade to enhance the cyber security capabilities and assistance provided to Australians through the Australian Signals Directorate and the Australian Cyber Security Centre.

The CESAR package has been designed to boost protection and cyber resilience for all Australians, from individuals and small businesses through to the providers of critical services.

s. 7(2A)

[redacted]

- o This measure compliments reforms that will give our law enforcement agencies increased ability to identify and disrupt cybercrime.

- Over $35 million to deliver a new cyber threat-sharing platform, enabling industry and government to share intelligence about malicious cyber activity, and block emerging threats in near real-time
    - o This measure will be critical to the broader measures to enhance the security of our critical infrastructure

- Over $12 million towards new strategic mitigations and active disruption options, enabling ASD and Australia's major telecommunications providers to prevent malicious cyber activity from ever reaching millions of Australians across the country by blocking known malicious websites and computer viruses at speed.

s. 7(2A)

[redacted]

s. 7(2A)

[redacted]