[SEC=OFFICIAL]

Active Cyber Defence Alliance

Protecting Critical Infrastructure and Systems of National Significance - Consultation Paper

A document developed by the Active Cyber Defence Alliance
Submission version as at 26 November 2020

A document developed by the Active Cyber Defence Alliance
Written by Helaine Leggat
27 November 2020

Incident Response Guide - Ransomware Attack

Who is the Active Cyber Defence Alliance (ACDA)?

The Active Cyber Defence Alliance (ACDA) is a special interest group comprised of industry, academic and government stakeholders whose aim is to foster awareness, adoption and capability in Active Cyber Defence practices across Australia with the goal of lifting Australia's cyber resilience.

Active Cyber Defence Alliance (ACDA) Cyber Strategy Group:

Lead Author
Helaine Leggat
Attorney at Law – ICT Legal Consulting

Debbie Lutter
CEO - AUSCSEC

Andrew Cox
CEO – Avantgard Pty Ltd

Francis Cox
Compliance Consultant

Ben Whitham
Founder and Director - Penten

John Powell
Principal Consultant for Cyber Security Qld – Telstra Purple

Duncan Unwin
Managing Director – Tobruk Security

Phillip Moore
Technical Manager – Avantgard Pty Ltd

Robert Neely
Partner – Lander & Rogers

Overview of Active Cyber Defence

Active Cyber Defence employs cyber intelligence, deception, active threat hunting and lawful countermeasures to detect and respond to malicious activity sooner and potentially more effectively than is possible with passive defence. While the tools and techniques of Active Cyber Defence have been in limited use for decades, they are becoming increasingly popular due to their enablement by technological growth and challenges with traditional approaches.

Active cyber security measures provide a complementary strategy to traditional, passive cyber defence, which relies on conventional cyber security practices such as network hygiene, firewalls, identity and access management, virus filters, good user behaviour, etc. Passive cyber defence has proven difficult to deliver in practice, and by itself, unable to prevent the continued growth in data leakage and incursions by cyber criminals and state actors.

While Active Cyber Defence, by its name, prefers a more dynamic set of controls, it excludes offensive cyber actions, which are the sole domain of authorised government agencies, although it could include mechanisms to enable potential responses by such agencies if enabled by the Security Legislation Amendment (Critical Infrastructure) Bill 2020 [Exposure draft].

Summary of Recommendations

A summary of recommendations is included in the table below on page 15, and at 10 and 11 below. Capitalised terms in the text are defined in the Bill.

Introduction

Protecting Critical Infrastructure and Systems of National Significance – Exposure Draft Bill

The Australian Government is committed to protecting the essential services all Australians rely on by uplifting the security and resilience of critical infrastructure and systems of national significance.

The Government has asked for feedback on its approach for developing an enhanced critical infrastructure security framework, specifically in relation to the *Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill* 2020 (the **Bill**).

The Active Cyber Defence Alliance Response

1. The ACDA offers the following feedback.

1.1. The Active Cyber Defence Aiilance (**ACDA)** believes that the adpotion of Active Cyber Defence (**ACD**) will greatly enhance the ability of the Australian Government to achieve the aims of the Bill, including:

1.1.1. An effective Positive Security Obligation for critical infrastructure, including a risk management program, to be delivered through sector-specific requirements, and mandatory cyber incident reporting;

1.1.2. enhanced cyber security obligations and cyber defensive capabilities for those assets most important to the nation, described as systems of national significance; and

1.1.3. effective provision of government assistance to relevant entities managing critical infrastructure sector assets in response to significant cyber attacks that impact on Australia's critical infrastructure assets and capability.

1.2. Furthermore, the ACDA believes that the adoption of Active Cyber Defence will provide Government and the private sector with a clear, effective, consistent and proportionate approach to cyber defence of critical infrastructure, systems of national significance, and critical infrastructure sector assets, by , inter alia, helping to establish new norms of behaviour through prescribed rules, which will be co-designed between industry and government.

1.2.1. While the Government has at its disposal resources and powers designed to ensure that Ausralia does not suffer a catastrophic cyber attack, it is essential that the capability and resources of the private sector be brought to bear, because it is not possible for the Government to provide direct assistance to industry in every instance of serious cyber security incident. The current draft legislation provides a binary choice in each incident between an essentially passive cyber defence and a highly offensive approach utilising all the powers of the Austalian Signals Directorate. We

propose a proportional continuum of active cyber defence and lawful counter meaures be mandated be up to the threshold of a declared cyber emergency.

Approach to the ACDA Response in this document

2. In this document we will:

2.1. Explain Active Cyber Defence and how it can assist the Government achieve the objectives of the Bill.

2.2. Provide details on Active Cyber Defence and lawfulness.

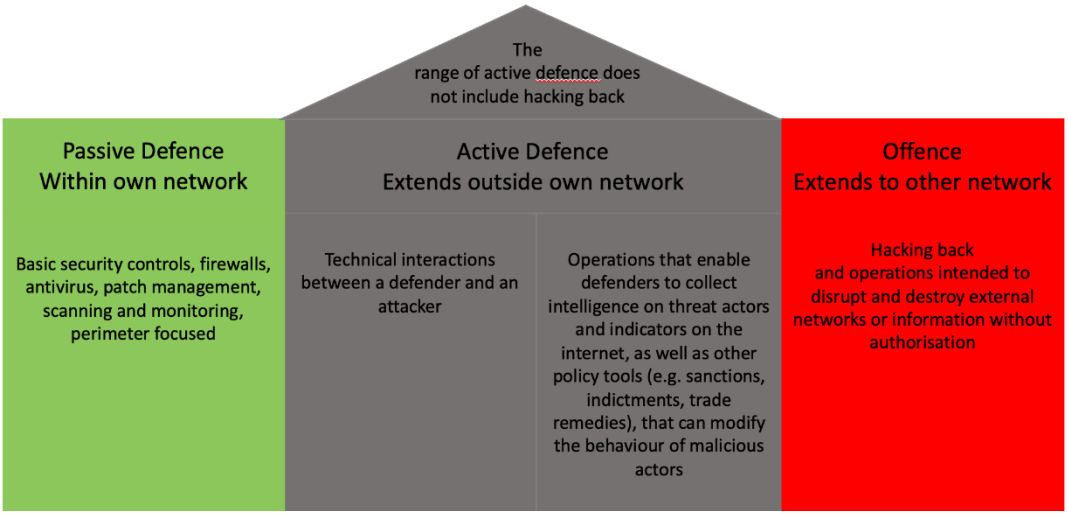
2.3. Identify where Active Cyber Defence alligns to provisions in the Bill and provide views

What is Active Cyber Defence and how can it assist the Government achieve its vision and objectives?

3. Active Cyber Defence employs cyber intelligence, deception and active threat hunting to detect malicious activity sooner and more reliably than is possible with passive defence. Passive defence relies on conventional cybersecurity practices such as network hygiene, firewalls, virus filters ,good user behaviour etc. By itself passive cyber defence has proven to be ineffective against sophisticated attacks. Active cyber defence excludes offensive cyber actions which are the sole domain of authorised government agencies, although it could include mechanisms to coordinate potential responses by such agencies

3.1. Passive Defence, Active Defence and Offence

Figure 1 Active Cyber Defence Framework



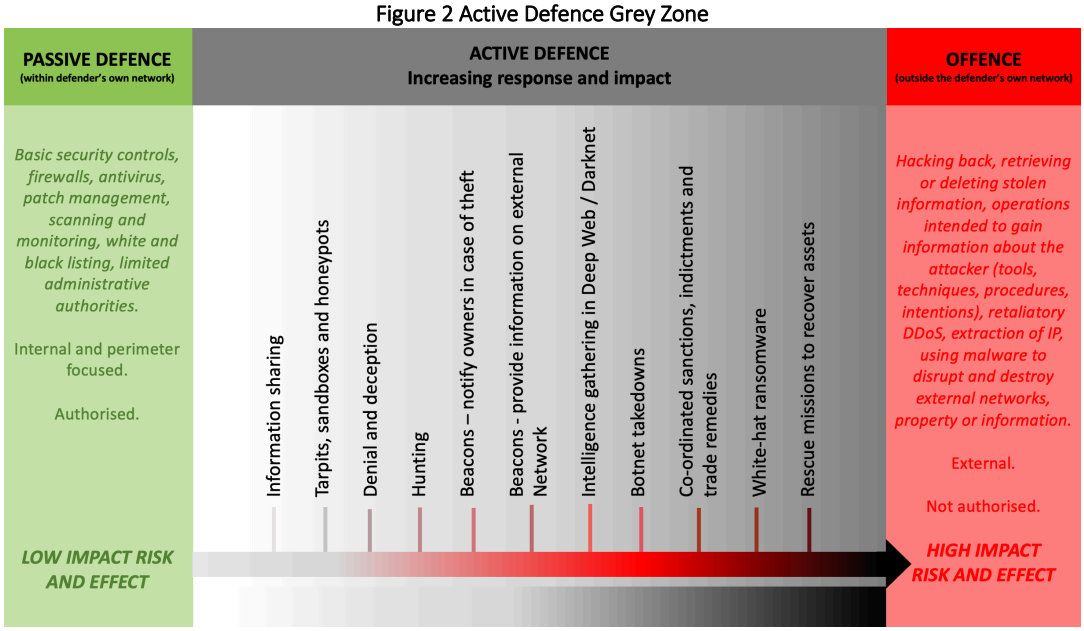
3.2. Traditional passive defence responses are shown in the green zone on the left the diagram above.

3.3. Offence – the sole domain of authorised government agencies - is shown on the red zone on the right side of the diagram. See detail in Fig 2 below.

3.4. Active Cyber Defence is shown on the grey zone between passive defence and offence.

4. The 'Grey Zone' of Active Defence

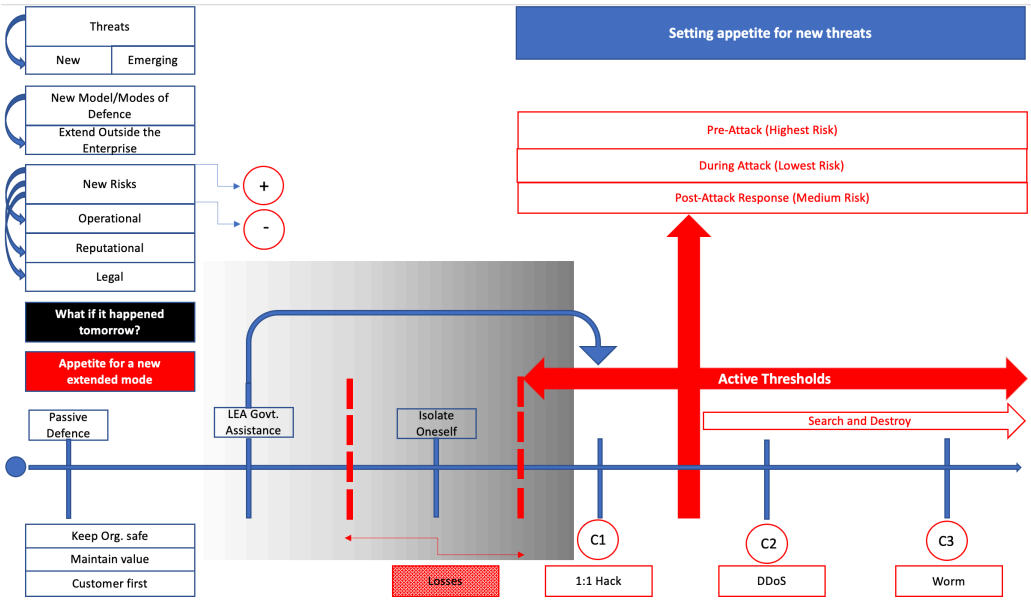
Figure 2 Active Defence Grey Zone



4.1. Possible Active Cyber Defence responses are shown in the diagram above[1]. See detail at 8 below.

4.2. The Risk and Threat Continuum

Figure 3 The Risk and Threat Continuum



4.2.1. The diagram shows how Active Cyber Defence responses become increasingly the domain of authorised government agencies as they move from passive defence to offence. The responses are detailed in 8.5 below.

4.2.2. The diagram shows how the private sector can be usefully empowered to assist government in the grey zone, prior to the Government providing assistance.

Active Cyber Defence – details and lawfulness

5. Active Cyber Defence is a proactive cyber defence posture that involves the responses listed at 8.5.1 to 8.5.12 below. Check numbers

6. Active Cyber Defence - The Issue

[1] The diagram is an adaptation from on in "Into the Gray Zone". The Private Sector and Active Defense against Cyber Threats. Centre for Homeland Security. The George Washington University. Project Report October 2016.

6.1. Active Cyber Defence responses involve access to information and information systems. Specifically, whether access is lawful.

7. Active Cyber Defence – Lawfulness

7.1.1. The lawfulness, of Active Cyber Defence rests upon whether the access to information and information systems is authorised or not.[2] Unauthorised access in not lawful.

7.1.2. Because Active Cyber Defence is about collecting intelligence and information on information systems, access to information and to information systems is a *sine qua non* to ACD responses.

7.1.3. Authorisation and lawfulness is primarily regulated under the following Australian Statutes,[3] and their State and Territory equivalents:

a. Telecommunications law (including interception and access);

b. *The Criminal Code*; and

c. Data Surveillance law.

8. Active Cyber Defence - Responses

8.1. A summary of Active Cyber Responses is set out below. The lower the number (8.5.1), the more likely the response is to be lawful. The higher the number (8.5.12), the higher the risk of the response being unlawful when carried out by a private sector entity or state government without the assistance of law enforcement or intelligence services.

8.2. The lower the number, the more compelling it is that these responses are adopted by private sector entities and state government. Not to do so could be a failure in due diligence and care, because these responses are now best practice. In the view of the ACDA the responses in 8.5.1 to 8.5.9 should be made positive obligations.

8.3. The higher the number, the more compelling it is that the responses are conducted with law enforcement/national security assistance. In the view of the ACDA the

[2] See *Criminal Code Act 1995* (Cth) Pt 10.7; *Telecommunications (Interception and Access) Act 1979* (Cth).
[3] Numerous other laws apply, specifically national intelligence and law enforcement, privacy and others, but for the purpose of this response, I am simplifying. The issue is to separate the executive powers of law enforcement from the legitimate actions by the private sector/state government.

responses in 8.5.10 to 8.5.12 should be made by the private sector with Government assistance, or by Government alone, depending on the circumstances.

8.4. Lawfulness of an Active Cyber Defence response also depends upon timing and proportionality. Different rules apply to a response that is before, during or after the attack. A raft of Australian and international legal precedent exists to determine how the ACD positive obligations can be adopted into the provisions of Bill. Legal precedent creates certainty and will assist in establishing new norms of behaviour in cyberspace, raising the bar to Australia as a target to malicious actors.

8.5. The Range of Active Cyber Defence Responses

8.5.1. *Information Sharing* - The sharing of actionable cyber threat indicators, mitigation tools, and resilience strategies between defenders to improve widespread situational awareness and defensive capabilities.

8.5.2. *Tarpits, Sandboxes & Honeypots* - Technical tools that respectively slow malicious actors to a halt at a network's perimeter, test the legitimacy of untrusted code in isolated operating systems, and attract malicious actors to decoy, segmented servers where they can be monitored to gather intelligence on malicious actor behaviour.

8.5.3. *Denial & Deception* - Preventing adversaries from being able to reliably access legitimate information by mixing it with false information to sow doubt and create confusion among malicious actors.

8.5.4. *Hunting* - Rapidly enacted procedures and technical measures that detect and surgically evict adversaries that are present in a defender's network after having already evaded passive defences.

8.5.5. *Beacons (Notification)* - Pieces of software or links that have been hidden in files and send an alert to defenders if an unauthorised user attempts to remove the file from its home network.

8.5.6. *Beacons (Information)* - Pieces of software or links that have been hidden in files and, when removed from a system without authorisation, can establish a connection with and send information to a defender with details on the structure and location of the foreign computer systems it traverses.

8.5.7. *Intelligence Gathering in the Deep Web/Dark Net* - The use of human intelligence techniques such as covert observation, impersonation, and misrepresentation of assets in areas of the Internet that typically attract malicious cyber actors in order to gain intelligence on malicious actor motives, activities, and capabilities.

8.5.8. *Botnet Takedowns* - Technical actions that identify and disconnect a significant number of malware-infected computers from the command-and-control infrastructure of a network of compromised computers.

8.5.9. *Honeyrecords (Information)* - Synthetically generated data records/documents containing unique code (fingerprint) that can be detected in a scan of the deep, dark and surface web. Honeyrecords provide positive evidence of data theft and give information on what data was stolen and when it was stolen.

8.5.10. *Coordinated Sanctions, Indictments & Trade Remedies* - Coordinated action between the private sector and the government to impose costs on known malicious cyber actors by freezing their assets, bringing legal charges against them, and enforcing punitive trade policies that target actors or their state sponsors.

8.5.11. *White-hat Ransomware* - The legally authorised use of malware to encrypt files on a third party's computer system that contains stolen information in transit to a malicious actor's system. Public-private partners then inform affected third parties that they have been compromised and are in possession of stolen property, which they must return in order to regain access to their files.

8.5.12. *Rescue Missions to Recover Assets* - The use of hacking tools to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. Rarely successful.

9. Other Factors to Consider

9.1. Consent

9.1.1. Consent makes access and in many cases the response itself lawful. There are many legitimate ways of getting consent.

9.2. Self-defence

9.2.1. Self-defence has been recognised for thousands of years in most legal systems. Just as the concept of 'unauthorised access' was a re-interpretation of 'trespass' in property law,[4] it is logical that the principles of self-defence might be re-interpreted from lawful defence on property and premises, to lawful defence on a network. See for example 9.2.1 below.

9.2.1.1. Self -Defence - *Criminal Code Act 1995* (Cth)

S 4 – Definitions: **'**property' includes:
(a) real property; (b) personal property; (c) money; (d) a thing in action or other intangible property; (e) electricity; and (f) a wild creature that is tamed / kept.

Division 10 - Circumstances involving external factors. 10.4

Self-defence
(1) A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence in self-defence.
(2) A person (includes a juristic person) carries out conduct in self-defence if and only if he or she believes the conduct is necessary:

(a) to defend himself or herself or another person; … or
(c) to protect property from unlawful appropriation, destruction,

[4] Recognised a criminal offence in the Budapest Convention on Cybercrime and adopted into the national legal systems of signatory countries – in Australia, the *Criminal Code Act 1995* (Cth).

damage or interference; ...
and the conduct is a reasonable response in the circumstances as he or she perceives them.

(3) This section does not apply if the person uses force that involves the intentional infliction of death or really serious injury.

CAN INJURE PEOPLE AND PROPERTY, BUT CANNOT CAUSE DEATH IN THE DEFENCE OF PROPERTY

10. The Active Cyber Defence Proposition

10.1. 20 years ago, the world recognised electronic transactions and communications through UNCITRAL[5] which recognised and facilitated a new legal basis for the world to co-operate. Now it is time that we agree what constitutes reasonable behaviour in cyberspace in the defence of Australia and its critical infrastructure, systems of national significance, and critical infrastructure sector assets.

10.2. The ACDA proposition is that there is sufficient commonality in the national laws of many countries (especially Australia and Australian allies), and sufficient legal precedent in numerous national legal systems to identify what can best be the foundation for new norms in cyberspace through inclusion of ACD responses in the Bill.

11. ACDA Views

11.1. Where the Government cannot easily adpot the ACD responses into the Bill, the view of the ACDA is that Government should:

11.1.1. Clarify through legislative and executive action:

11.1.1.1. That Australian laws apply to cyberspace;

[5] UNCITRAL has been responsible for one convention and two model laws which have shaped the modernisation and harmonisation of electronic commerce: https://uncitral.un.org/

11.1.1.2. Which Active Cyber Defence responses are lawful.

11.1.1.3. Establish whether the principles of self-defence apply to a network as they do to a property and premises.

11.1.1.4. Confirm that the principles and defences applicable in burglary and hot pursuit apply to the recovery of data in the process of exfiltration.

11.1.1.5. Empower the private sector and state governments through existing law – for example, telecommunications law, intelligence law (*ASIO Act*), and even new statutes such as the *Security Legislation Amendment Bill 2020* – to enable certain qualified persons in qualified industry sectors to undertake Active Cyber Defence responses. In simple terms, this means 'delegating' authority to spread the load which otherwise falls on Government. This will raise the cost of attacking Australia at scale.

11.1.1.6. Mandate certain Active Cyber Defence responses through inclusion in the Bill, to embed preparation, prevention and mitigation activities into the business-as-usual operation of critical infrastructure assets, ensuring that the resilience of essential services is strengthened and providing greater situational awareness of threats to critical infrastructure assets

Active Cyber Defence alignment with provisions in the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

12. The table below includes a summary of provisions from the Bill and the relevant Active Cyber Defence responses.

Section	**Content**	**Active Cyber Defence Response/Comment**
Definitions		
Section 12M - Meaning of cyber security incident.	A cyber security incident is one or more acts, events or circumstances involving any of the following: (a) unauthorised access to:	Consider – which Active Cyber Defence responses can be employed against which incidents. Align these for lawfulness.

	(i) computer data; or (ii) a computer program; (b) unauthorised modification of: (i) computer data; or (ii) a computer program; (c) unauthorised impairment of electronic communication to or from a computer; (d) unauthorised impairment of the availability, reliability, security or operation of: (i) a computer; or (ii) computer data; or (iii) a computer program.	
Section 12N - Meaning of unauthorised access, modification or impairment	(1) For the purposes of this Act: (a) access to: (i) computer data; or (ii) a computer program; or (b) modification of: (i) computer data; or (ii) a computer program; or (c) the impairment of electronic communication to or from a computer; or (d) the impairment of the availability, reliability, security or operation of: (i) a computer; or (ii) computer data; or (iii) a computer program; by a person is unauthorised if the person is not entitled to cause that access, modification or impairment. (2) For the purposes of subsection (1), it is immaterial whether the person can be identified. (3) For the purposes of subsection (1), if: (a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and (b) the person does so: (i) under a warrant issued under a law of the Commonwealth, a State or a Territory; or (ii) under an emergency authorisation given to the person under Part 3 of the Surveillance	Which Active Cyber Defence responses will not be regarded as unauthorised access? The Bill should mandate some as positive obligations, especially to enable certain qualified persons in qualified industry sectors—Critical Infrastructure - to undertake Active Cyber Defence responses. i.e appoint qualified and capable people and organisations to undertake some of the tasks traditionally reserved for Government and LEA to spread the load in protecting Australia. Amend this section accordingly.

	Devices Act 2004 or under a law of a State or Territory that makes provision to similar effect; or (iii) under a tracking device authorisation given to the person under section 39 of the *Surveillance Devices Act 2004*; or (iv) in accordance with a technical assistance request; or (v) in compliance with a technical assistance notice; or (vi) in compliance with a technical capability notice; the person is entitled to cause that access, modification or impairment.	
Section 12P Examples of responding to a cyber security incident	The following are examples of responding to a cyber security incident: (a) if the incident is imminent—preventing the incident; (b) mitigating a relevant impact of the incident on: (i) a critical infrastructure asset; or (ii) a critical infrastructure sector asset; (c) if a critical infrastructure asset or a critical infrastructure sector asset has been, or is being, affected by the incident—restoring the functionality of the asset.	Mandate appropriate Active Cyber Defence responses.
30CN Definition: Cyber security exercise	(1) A cyber security exercise is an exercise: a) that is undertaken by the responsible entity for a system of national significance; and b) that relates to the system; and c) that either: (i) relates to all types of cyber security incidents; or (ii) relates to one or more specified types of cyber security incidents; and d) if the exercise relates to all types of cyber security incidents—the purpose of which is to: (i) test the entity's ability to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and	Mandate appropriate Active Cyber Defence response exercises (scenario planning), appropriate to a risk management program. i.e What can lawfully be done, when and by whom?

	(ii) test the entity's preparedness to respond appropriately to all types of cyber security incidents that could have a relevant impact on the system; and (iii) test the entity's ability to mitigate the relevant impacts that all types of cyber security incidents could have on the system; and e) if the exercise relates to one or more specified types of cyber security incidents—the purpose of which is to: (2) (i) test the entity's ability to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and (ii) test the entity's preparedness to respond appropriately to those types of cyber security incidents that could have a relevant impact on the system; and (iii) test the entity's ability to mitigate the relevant impacts that those types of cyber security incidents could have on the system; and (f) that complies with such requirements (if any) as are specified in the rules. (2) Requirements specified under paragraph (1)(f): (a) may be of general application; or (b) may relate to one or more specified systems of national significance; or (c) may relate to one or more specified types of cyber security incidents.	
Section 4 Simplified outline of this Act		
	This Act creates a framework for managing risks relating to critical infrastructure. The framework consists of the following: (a) the keeping of a register of information in relation to critical infrastructure assets (the register will not be made public); (b) requiring the responsible entity for one or more critical infrastructure assets to have, and comply with, a critical infrastructure risk management program;	Apply each of the Active Cyber Defence responses discussed above to the requirements specified in the Bill. Formally and legally provide certainty in the Bill as to what Active Cyber Defence responses can be carried out by which authorised and

	(c) requiring notification of cyber security incidents; (d) imposing enhanced cyber security obligations that relate to systems of national significance; (e) requiring certain entities relating to a critical infrastructure; (f) allowing the Minister to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security; (g) allowing the Secretary to require certain entities relating to a critical infrastructure asset to provide certain information or documents; (h) setting up a regime for the Commonwealth to respond to 2 serious cyber security incidents; (i) allowing the Secretary to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset. Certain information obtained or generated under, or relating to the operation of, this Act is protected information. There are restrictions on when a person may make a record of, use or disclose protected information. Civil penalty provisions of this Act may be enforced using civil penalty orders, injunctions or infringement notices, and enforceable undertakings may be accepted in relation to compliance with civil penalty provisions. The Regulatory Powers Act is applied for these purposes. Certain provisions of this Act are subject to monitoring and investigation under the Regulatory Powers Act. Certain provisions of this Act may be enforced by imposing a criminal penalty. The Minister may privately declare an asset to be a critical infrastructure asset. The Minister may privately declare a critical infrastructure asset to be a system of national significance. The Secretary must give the Minister reports, for presentation to the Parliament, on the operation of this Act.	capable persons and organisations. Clarify the lawfulness and positive obligation of each Active Cyber Defence response wrt each requirement in the framework. Provide for penalties where organisations do not meet the necessary Active Cyber Defence response levels. Provide for the physical and mental elements of failure to act (intention and negligence). The Minister and the Secretary should make declarations to include Active Cyber Defence responses as positive obligations.

Part 2A – Critical infrastructure risk management programs		
30AA Simplified outline of this Part 5	The responsible entity for one or more critical infrastructure assets must have, and comply with, a critical infrastructure risk management program. The purpose of a critical infrastructure risk management program is to do the following for each of those assets: (a) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; (b) so far as it is reasonably possible to do so—minimise or eliminate any material risk of such a hazard occurring; (c) mitigate the relevant impact of such a hazard on the asset. A responsible entity must give an annual report relating to its critical infrastructure risk management program. If the entity has a board, council or other governing body, the annual report must be signed by each member of the board, council or 2other governing body.	The critical infrastructure risk management program must be linked to appropriate Active Cyber Defence responses – which are clearly defined and mandated. Provide for positive obligations wrt Active Cyber Defence response planning and exercises.
Part 2B—Notification of cyber security incidents		
30BA Simplified outline of this Part 4	If a cyber security incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident.	Apply the appropriate Active Cyber Defence response – specifically in this case – identify what constitutes lawful information sharing that does not contravene public or private sector information classification restrictions. This requires, *inter alia*, clarification of privacy vs Surveillance legislation. The Bill must stipulate what Active Cyber Defence responses are lawful under what circumstances.
Part 2C—Enhanced cyber security obligations		
Division 1—Simplified outline of this Part 30CA - Simplified outline of this Part	This Part sets out enhanced cyber security obligations that relate to systems of national significance. The responsible entity for a system of national significance may be subject to statutory incident response planning obligations. The responsible entity	These statutory incident response planning obligations must include more pro-active Active Cyber Defence responses, including those to be undertaken with LEA and

	for a system of national significance may be required to undertake a cyber security exercise. The responsible entity for a system of national significance may be required to undertake a vulnerability assessment. If a computer is a system of national significance, or is needed to operate a system of national significance, the responsible entity for the system may be required to: (a) give ASD periodic reports of system information; or (b) give ASD event-based reports of system information; or (c) install software that transmits system information to 2 ASD.	National security agencies (on the right side of the grey zone). Provide for positive obligations wrt Active Cyber Defence response planning and exercises.
Subdivision B—System information software 30DJ - Secretary may require installation of system information software	Scope (1) This section applies if: (a) a computer: (i) is needed to operate a system of national significance; or (ii) is a system of national significance; and (b) the Secretary believes on reasonable grounds that the responsible entity for the system of national significance would not be technically capable of preparing reports under section 30DB or 30DC consisting of information that: (i) relates to the operation of the computer; and (ii) may assist with determining whether a power under this Act should be exercised in relation to the system of national significance; and (iii) is not personal information (within the meaning of the Privacy Act 1988). Requirement (2) The Secretary may, by written notice given to the entity, require the entity to: (a) both: (i) install a specified computer program on the computer; and (ii) do so within the period specified in the notice; and	The Secretary should by written notice given to the entity, require the entity to undertake certain Active Cyber Defence responses that clearly specify that the actions mandated are lawful, including wrt timing and proportionality. Note that the definitions included above provide an easy mechanism for including lawfulness of the Active Cyber Defence responses.

	(b) maintain the computer program installed in accordance with paragraph (a); and (c) take all reasonable steps to ensure that the computer is continuously supplied with an internet carriage service that enables the computer program to function. (3) A notice under subsection (2) is to be known as a system information software notice. (4) In deciding whether to give a system information software notice to the entity, the Secretary must have regard to: (a) the costs that are likely to be incurred by the entity in complying with the notice; and (b) such other matters (if any) as the Secretary considers 6 relevant. (5) A computer program may only be specified in a system information software notice if the purpose of the computer program is to: (a) collect and record information that: (i) relates to the operation of the computer; and (ii) may assist with determining whether a power under this Act should be exercised in relation to the system of national significance; and (iii) is not personal information (within the meaning of the Privacy Act 1988); and (b) cause the information to be transmitted electronically to ASD.	
Division 6—Designated officers 30DQ Designated officer	(1) A designated officer is an individual appointed by the Secretary, in writing, to be a designated officer for the purposes of this Act. (2) The Secretary must not appoint an individual under subsection (1) unless: (a) the individual is an APS employee in the Department; or (b) the individual is a staff member of ASD (within the meaning of the Intelligence Services Act 2001).	The Secretary should appoint designated officers within private sector entities to lawfully undertake and be responsible for Active Cyber Defence responses. This can be achieved through the Bill, and other legislation – viz: telecommunications law (extend the power and authority of the 'network operator'), and the ASIO Act (appoint ASIO 'Affiliates').
35AAB Liability	(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in	Clarify the lawfulness and applicability of self-defence to cyberspace.

	compliance with a direction under subsection 32(2). (2) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1) of this section.	Specifically – does self-defence and the protection of property (CI assets, information and systems) apply equally as in other applications provided for in the Criminal Code Act 1995, tort and common law? Persons authorised under the Bill should not be liable or able to be prosecuted for defending a CI assets, information and systems where the Active Cyber Defence responses are clarified and specified in the Bill as nationally and internationally within the boundaries of lawful self-defence.
Part 3A—Responding to serious cyber security incidents		
Division 1—Simplified outline of this Part 22 35AA	This Part sets up a regime for the Commonwealth to respond to serious cyber security incidents. If a cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset, the Minister may, in order to respond to the incident, do any or all 2 of the following things: (a) authorise the Secretary to give information-gathering directions to a relevant entity for the asset; (b) authorise the Secretary to give an action direction to a relevant entity for the asset; (c) authorise the Secretary to give an intervention request to the authorised agency. An information-gathering direction requires the relevant entity to give information to the Secretary. An action direction requires the relevant entity to do, or refrain from doing, a specified act or thing. An intervention request is a request that the authorised agency do one or more specified acts or things in relation to the asset.	This Part should include private sector Active Cyber Defence responses, set up with the regime for the Commonwealth to respond to serious cyber security incidents. These actions are those to the right- hand side of the Active Cyber Defence response and threat and risk continuum. The Bill should provide for a clear delineation of: 1. What Active Cyber Defence responses must be employed by CI organisations as positive obligations; 2. What Active Cyber Defence responses may be lawfully employed by CI organisations; and 3. What Active Cyber Defence responses must be employed by CI organisations; in conjunction with LEA and other

		Government agencies. *ALL THESE ACTIONS MUST BE CLARIFIED IN THE BILL.* *THERE IS NO TIME ONCE AN ATTACK HAS COMMENCED FOR AN ORGANSATION TO APPROACH A COURT FOR INJUNCTIVE OR SIMILAR RELIEF.*
Part 6A—Declaration of systems of national significance by the Minister		
Division 1—Simplified outline of this Part 4 52A	The Minister may privately declare a critical infrastructure asset to be a system of national significance. The Minister must notify each reporting entity for an asset that is a declared system of national significance. If a reporting entity for an asset that is a declared system of national significance ceases to be such a reporting entity, or becomes aware of another reporting entity for the asset, the entity must notify the Secretary. Note: It is an offence to disclose that an asset has been declared a system of national significance (see section 45).	These responses should be the same as those above. It is not practical to make it an offence to disclose that an asset has been declared a system of national significance – this goes to information sharing, and exceptions should be provided to allow for Active Cyber Defence responses.

Contact Details

Attention: Helaine Leggat
Active Cyber Defence Alliance
c/o ICTLC Australia
T: [redacted]
E: [redacted]

Alternative contact
Attention: Andrew Cox
Active Cyber Defence Alliance
c/o Avantgard Pty Ltd
T: [redacted]
E: [redacted]
Australia