Risk Leader® ARPI   GRPN Global Risk Policy Network   ARPI® Australian Risk Policy Institute

Submission by the Centre for Advanced Resilience and Risk Policy Studies (CARRPS™), the research component of the Australian Risk Policy Institute (ARPI®) - in response to an invitation by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) concerning the Review of Cyber Security Legislative Package 2024.

PARLIAMENT OF AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
PO Box 6021, Parliament House, Canberra ACT 2600 | Phone: (02) 6277 2360 | Email: pjcis@aph.gov.au | www.aph.gov.au/pjcis

Review of Cyber Security Legislative Package 2024
INVITATION TO MAKE A SUBMISSION

"The Cyber Security Legislative Package intends to implement seven initiatives under the 2023-2030 *Australian Cyber Security Strategy*, which aims to address legislative gaps to bring Australia in line with international best practice and help ensure Australia is on track to become a global leader in cyber security.

These measures are intended to address gaps in current legislation to:

- mandate minimum cyber security standards for smart devices;
- introduce mandatory ransomware reporting for certain businesses to report ransom payments;
- introduce 'limited use' obligations for the National Cyber Security Coordinator and the Australian Signals Directorate (ASD); and
- establish a Cyber Incident Review Board.

The package also intends to progress and implement reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act). These reforms are intended to:

- clarify existing obligations in relation to systems holding business critical data;
- enhance government assistance measures to better manage the impacts of all hazards incidents on critical infrastructure;
- simplify information sharing across industry and Government;
- introduce a power for the Government to direct entities to address serious deficiencies within their risk management programs; and
- align regulation for the security of telecommunications into the SOCI Act."

About the Australian Risk Policy Institute (ARPI®)

ARPI® is an independent, not-for-profit, incorporated association, promoting professional collaboration through a global network of influence (see www.arpi.org.au). ARPI® was formed to develop and promote risk policy innovation for anticipation and awareness, progressively missing from risk management programs.

ARPI® promotes leadership paradigm change to embrace risk policy reform, urgently required today to enable informed and pre-emptive decision-making, resilience and sustainability in the age of digital transformation and disruption often without notice and not at the same time.

ARPI®'s over-riding submission theme is the need for significant, ongoing enhancements to existing legislation as illustrated in the dot points above (and more) to which ARPI® will respond to only briefly, given time constraints on responding to the submission invitation. Equally important is that reform is urgently needed and recommended by ARPI® to adopt contemporary, holistic policy and strategic approaches in the consideration of risk, essential to meet both challenges and opportunities existing and foreseeable.

ARPI® presents integrated, whole-system, policy reform thinking, approaches and frames as follows:

1. Introduction of a Strategic Risk Policy® approach that doesn't rely on fundamentally out-of-date risk management concepts and processes which continue to fail around the world despite being considered 'best-practice'. We promote that risk adjustment starts with leadership paradigm change from siloed organisation-centric thinking and adopting the Strategic Risk Policy® approach of network-centric thinking. This is because irrefutably, information today resides in networks: the world being interconnected and interdependent like never before creating an information meta-grid.

Further, it is essential to recognise that today, risk is based in vulnerability and concerned with consequences. Consequences must govern leadership thinking so the focus needs to be on 'protection against' vulnerabilities – which we define as potential or possible strategic risks. Protection against vulnerabilities builds resilience, productivity and sustainability, reduces the number and severity of any risks from left-field. Such an approach overcomes reliance on managing existing risks, which carry a degree of probability of happening, because risk management continues to be too late, too little or not all. Discernment of risk and vulnerability is one of the greatest policy challenges in the world today.

Attached are two recent ARPI® publications illustrating vulnerability, potentiality and consequence. The global uptake of Strategic Risk Policy® is also illustrated through ARPI® being a Founding Partner in the global-scale Human Continuity Project™ to enhance resilience across ten areas of critical global infrastructure. Details can be found at www.eiscouncil.org including information about the *Resilient Renewable Society (R2S) Summit* held at the Imperial College London on 23 and 24 September 2024.

2. Data intelligence concepts and systems have passed the point where governance is coping using current approaches. Artificial Intelligence (AI), big data, quantitative modelling, quantum computing et al – have a significant common vulnerability – they cannot see let alone address 'totality of a situation', and most likely will never be able to do so. In addition, advanced research by CARRPS™ suggests an existential AI timeline exists of data intelligence conceptual and system failure that if not countered will cause, on a global scale, implosion of systems addressing critical infrastructure, increasingly being referred to as an existential global threat to society. It is authoritatively accepted that AI cannot solve AI's problems. The answer lies in identification, analysis, codification and measurement enabling systemisation of data outside the scope of AI. Thus, being able to see the totality of a situation. CARRPS™ is also conducting advanced research and validation in the science of Intelligence Augmentation (IA) involving 'Mixed-Mode' Qualitative-Quantitative integration.

3. Regulation, while a fundamental part of civil society and represented inter alia by standards which remain frameworks for minimum acceptable activity, has become increasingly lacking in effectiveness to address today's challenges many of which have not been seen before, some unimaginable, alongside an increasing societal lack of accountability, compliance and enforcement. Self-regulation has diminished in value and adoption. In keeping with the new approaches outlined above, regulation of at least the most sensitive areas of policy, must apply a greater emphasis on proscriptive regulation – performance-based

and outcomes focused – rather than merely relying on prescriptive regulation that is base-lined for today's critical needs.

Brief responses follow to the nine points outlined above from the Cyber Security Legislative Package 2024 – provided in the context of the immediately preceding policy reforms urged by ARPI®.
ARPI® is available to provide additional information to PJCIS via an in-person briefing.

"These measures are intended to address gaps in current legislation to":

- mandate minimum cyber security standards for smart devices;
  - ARPI® comment: This must be viewed in the context of the whole IT/technology landscape which is inter-related so must be regulated in an enforceable, performance-based manner as well as the proposed benchmark prescriptive standard. Threats and threat actors are well ahead of routine 'prescriptive' regulation.

- introduce mandatory ransomware reporting for certain businesses to report ransom payments;
  - ARPI® comment: Cause and effect are inseparable in policy design including when considering ransomware. This measure is positive but again must be viewed from a whole-system perspective.

- introduce 'limited use' obligations for the National Cyber Security Coordinator and the Australian Signals Directorate (ASD); and
  - ARPI® comment: Leadership and security paradigms need to change from organisation-centric to network-centric thinking, approaches and frames. This is essential to protect against risk at the earlier point of (defined) vulnerability, and to identify consequences of unawareness. This is an area of research and innovation by ARPI® and CARRPS™. Enshrining silos would be disadvantageous.

- establish a Cyber Incident Review Board.
  - ARPI® comment: This should be a Total Quality Review process to ensure that adequate measures are in place to identify and protect against cyber vulnerabilities rather than trying to mitigate cyber risks or respond to crises, most of which are foreseeable if the approach to risk and intelligence is advanced for today's security and resilience needs.

The package also intends to progress and implement reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act). These reforms are intended to:

- clarify existing obligations in relation to systems holding business critical data;
  - ARPI® comment: An integrated approach is recommended based on discerning vulnerability and risk which remains one of the greatest policy challenges worldwide.

- enhance government assistance measures to better manage the impacts of all hazards incidents on critical infrastructure;
  - ARPI® comment: Priority should focus on 'protection against vulnerabilities' which reduces the severity and frequency of identifying or managing risks or crises, which is often too little or too late or not at all. 'More of the same but better', whilst incremental, must be replaced by a change in thinking and approaches.

- simplify information sharing across industry and Government;
  - ARPI® comment: Information today resides in networks; a meta-grid. Society is interconnected and interdependent like never before. Governments are often the last to

know. Moving to a secure, network-centric approach, along with advancing risk thinking to the point of vulnerability, through the work of the Global Risk Policy Network established by ARPI®, are achieving 'up-front' resilience and sustainability. ARPI® is a Founding Partner with the Electric Infrastructure Security Council in the global-scale Human Continuity Project™ to enhance resilience across ten primary areas of critical infrastructure (see www.eiscouncil.org).

- introduce a power for the Government to direct entities to address serious deficiencies within their risk management programs; and
  - ARPI® comment: This is a fundamental policy reform point. Daily life proves beyond doubt that society can no longer rely on even the best risk management programs and processes. To continue to do so, is a 'temporary illusion.' Leaders need 'anticipation and awareness,' hence new thinking, new approaches and new frames which are available and must be adopted to drive leadership paradigm change needed to enable informed and pre-emptive decision-making, in today's transformative and disruptive world.

    Risk management programs, processes and registers will remain a databank as the world must and will transition to the new trilogy of 'strategic leadership ⇔ vulnerability awareness ⇔ informed and pre-emptive decision making' – to achieve effective resilience.

    Legislative changes are recommended to adopt the principles espoused in Strategic Risk Policy® to require a focus on mandatory reporting to government, by government and non-government sectors, of 'vulnerability' not just 'risk'. At present, reporting 'risk' which is undefined in the legislation is a problem itself, as it will continue to be 'too little, too late or not all' and functionally fatal for resilience of critical infrastructure.

- align regulation for the security of telecommunications into the SOCI Act."
  - ARPI® comment: Regulation must adopt a whole-system approach hence all areas of infrastructure must be aligned in basics, allowing for additional sector nuances. More so even, a more advanced form of regulation is required beyond the traditional, lowest-common-denominator, 'prescriptive' approach – common in standards (guidelines) and legislation.

    Whilst prescription was applicable and effective in the past, today's transformative and disruptive world, with lower accountability, compliance and enforcement, must introduce a 'higher-level' of regulation, namely, outcomes-focused, performance and governance based, as already existing in some areas of law reform, namely, 'proscription.'

    Ultimately, prescriptive regulation will be substantially reduced globally to form baseline guidelines, with proscriptive approaches necessary for resilience of critical global infrastructure. ARPI®'s Centre for Advanced Resilience and Risk Policy Studies (CARRPS™) priorities include advanced approaches to protect against vulnerabilities; identifying and developing solutions to close gaps, and protecting against the dangers of uncontrolled and inappropriate use of AI. Both of these areas increasingly represent significant vulnerabilities and if they remain unprotected, may bypass 'risks' to become existential crises.

    ARPI® has recently contributed its 'risk innovation' theory and practice involving whole-system thinking in two significant cyber security areas. The first being a bilateral Australia-India project developing an Ethical Governance 6G Frame, and second, another globally urgent area being the safe use of social media through regulatory reform outlined above.

    Proscriptive regulation that is outcomes-focused and performance-based is considered by ARPI® and its Global Risk Policy Network as the only practicable solution. Viewing the social media frame 'in pieces' would remain a band-aid approach; reactive, linear, siloed, unenforceable and not constitute the best solution for industry and consumers.

Risk Leader®
ARPI

GRPN
Global Risk Policy Network

ARPI®
Australian Risk Policy Institute

Contacts:
Tony Charge FARPI
ARPI® President and Chairman
[redacted]

Gill Savage FARPI
ARPI® Vice President, Global
Director, CARRPS™
[redacted]

19 October 2024

USRRPI
United States
Resilience & Risk
Policy Institute

ERPI
European Risk Policy Institute

UKRPN
United Kingdom Risk Policy Network

ACGRPN
Asian Centre for the Global Risk Policy Network

Centre for
Advanced
Resilience
and
Risk Policy
Studies

Risk Leader® ARPI

GRPN
Global Risk Policy Network

ARPI®
Australian Risk Policy Institute

WHY THE WORLD MUST VIEW CYBER RISK DIFFERENTLY

As the world slowly recovers from the CrowdStrike failure impacting Microsoft this week which quickly dominoed into a global meltdown of essential IT services, ARPI urges all sectors of global society, particularly governing bodies and telcos, to think past immediate 'system recovery and damage control' to understand how and why it happened in a broader societal sense. Could anything have been done to protect society against this global vulnerability - and previous global vulnerabilities - which rapidly bypassed awareness and went straight to crises? Is there is similarity to continuing cyber-attacks, Covid, Global Financial Crisis, 9/11 and attempted political assassinations?

The way we live and work has changed rapidly this century, becoming interconnected and interdependent like never before, now a virtual meta-grid. Economic dominance prevails, product innovation remains unmatched by fit-for-purpose risk and reliance systems thinking, causing service and product delivery systems to be inherently vulnerable and subject to rapid deterioration.

IT systems innovation has not occurred in parallel with an essential progression and advancement of risk and resilience thinking, and whole systems approaches, to assure the meta-grid of dependence, that it is secure, safe, reliable and resilient. For example, was the upgrade (patch) by CrowdStrike examined for vulnerabilities (requiring protection against) before it was applied simultaneously across the world? If not, a compound or domino vulnerability was created.

An ARPI Principle states that 'Risk today is based in vulnerability, concerned with consequence.' Accordingly, resilience depends on looking for, identifying and protecting against vulnerabilities. Vulnerabilities being defined as potentiality or possibility of strategic risks.

Global leadership paradigm change is required urgently to transition **from** 'reaction and/or denial' which are often too little or too late by maintaining outdated silo or organization-centric thinking, **to a new leadership paradigm**, viewing the world in whole-systems – reflecting the meta-grid of interconnectedness and interdependence. This is the resilience key to identify presently 'hidden' vulnerabilities, visualize network consequences, and enable early executive action to protect against vulnerabilities. The result will be increasingly enhanced 'up-front' resilience of critical global infrastructure including water, electricity, gas, bushfires, floods, transport, communications, medicines and fuels. The global aim is redundant resilience.

ARPI as a global thought leader has developed Strategic Risk Policy® - www.arpi.org.au - which supports necessary leadership paradigm change to achieve vulnerability-protected infrastructure resilience. This will be illustrated by ARPI at The Resilient and Renewable Society (R2S) Summit at the Imperial College London on 23rd and 24th September this year – www.eiscouncil.org.

Contact: inquiry@arpi.org.au **21 July 2024**

Risk Leader®
ARPI

GRPN
Global Risk Policy Network

ARPI®
Australian Risk Policy Institute

ARPI Perspective – Top 10 Global Vulnerabilities – 7 July 2024

The Australian Risk Policy Institute (ARPI) as convenor of the Global Risk Policy Network (GRPN) announces the Top Ten Global Vulnerabilities in July 2024 identified through Strategic Risk Policy® foresight. ARPI's Pillar of Policy Reason is that 'Today, Risk is based in Vulnerability and concerned with Consequences.'

Vulnerability is defined as 'Potentiality or Possibility of Strategic Risk.' ARPI delivers contemporary thinking and approaches about risk to empower leaders to make informed and pre-emptive decisions, essential in today's transformative and disruptive world. Strategic Risk Policy® is Risk 4.0. It enables anticipation and alerts hence awareness – in time to 'protect against' vulnerabilities, whilst also building resilience. An ARPI Principle differentiates vulnerability from risk: 'Risk is the Consequence of the Conjunction of Vulnerability + Threat + Threat Actor.' Understanding the difference is one of the world's greatest policy challenges.'

ARPI proclaims that leadership paradigm change is needed from organisation-centric thinking and approaches to network-centric thinking and approaches because today, information resides in networks.

1. Consequence vector of interconnectedness and interdependence of Information Technology requires greater understanding and attention – the 'Red Dragon'.
2. Need to understand and accept the urgency of achieving 'Intelligence Equilibrium' between Artificial Intelligence (AI) and matters outside AI which constitute 'Intelligence Augmentation' (IA).
3. Radical political undercurrents operating internationally and nationally causing societal division, policy ambiguity, public chaos, crime unabated, abandoned governance, arguably to achieve State control based on misguided belief in a flawed 'New World Order.' The elephant in the global room.
4. Lack of strategic change leadership in society - skills, values, commitment, courage, resolve, presence and resilience to overcome multifarious challenges and undercurrents of destabilisation.
5. Exponential, weaponised multi-media communications – creating social fear, health deterioration, disrespect even disregard for law and order, and short-termism.
6. Delays in redressing global economic dominance resulting from failed Globalisation V1.
7. Lack of culture change necessary to achieve 'Redundant Resilience' of critical global infrastructure.
8. Difficulty in removing blockages to protect against the 'Risk of Rapid Deterioration' in society occurring anywhere, anytime, by any means, across the world.
9. Present volatility, inadequacy and inconsistency of unified decision-making by the new 'Convocation of Nations' to achieve and maintain economic, military and social stability - and sustainability.
10. Disrespecting lessons from history and misinterpreting science regarding 'cause and effect' of impactful changes in earth systems and mankind's proven ability to overcome challenges.