Protecting Critical Infrastructure and Systems of National Significance - Consultation Paper

PwC Submission September 2020

Table of Contents

Executive Summary

Our view on critical infrastructure security reforms

Securing the future economic prosperity of Australia

In an increasingly digitised and interconnected world, protecting Australia's critical infrastructure systems and services are more important than ever. 2020 has brought this into stark relief; demonstrating that disruption is a fact of life and is occurring with increasing frequency around the world. Both public and private sectors have simultaneously acknowledged the importance of strengthening resilience in the face of disruption and shocks, and this presents a window of opportunity for regulatory reform and to build new partnerships.

Whilst there are tremendous benefits from increasing digitisation and automation, the risk of disruption to our most critical services has increased. We can no longer rely on physical boundaries and geographic isolation to protect our most critical assets. Power grids can be controlled centrally from thousands of miles away; hospital life-support systems can be targeted through cyber attacks; transport vehicles are becoming autonomous and rely on machines to keep their occupants alive.

The recent bushfires and COVID-19 pandemic have highlighted significant challenges arising from sustained disruption to these types of services and supply chains. The complex dependencies between critical systems may be unknown until they are tested in a response scenario, such as fire damage to electricity networks impacting ATMs and telecommunications networks, increased threat to Australia's food and water security, and the flow-on impact to emergency responders.

These dynamic threats combined with the fragmented nature of critical infrastructure operators both locally and internationally, means the problem can only be tackled in an holistic multi-disciplinary fashion. Cyber, physical, personnel and supply chain risks will only continue to converge.

We believe that an enhanced regulatory framework for critical infrastructure will enable industry and government to work more effectively together to reduce risk of disruption from all hazards and threats, and enable rapid restoration of social and economic activities when a crisis evenuates. The framework will need to be tailored to specific sectors in line with global best practice but supported by universal principles underpinning the legislation. It is important the Government set the right tone when they launch the new reforms, specifically in regards to the cyber security responsibilities that belong to critical infrastructure entities, and the role that government plays from a risk management perspective.

PwC itself may not be considered a critical infrastructure operator, however, we do work with clients across the full spectrum of critical infrastructure industries and have played a pivotal role in the advancement of critical infrastructure security. We worked with AEMO, Home Affairs and the ACSC to develop the Australian Energy Sector Cyber Security Framework (AESCSF) in 2018 which we believe sets a great example on the private / public partnership needed to strengthen the resilience of our nation's most critical infrastructure assets. This submission paper includes our points of view and responses to consultation paper questions we feel we are best positioned to contribute to.

Who will the enhanced framework apply to?

We agree with the Government’s move to broaden the definition of critical infrastructure as outlined in the consultation paper. We believe there is also an opportunity to consider additional industry sectors that, if disrupted, could impact the future economic prosperity of Australia. The key areas to consider would be elements of the mining sector who contribute to some of our most critical exports (e.g. iron ore), and the manufacturing sector for the refinement / manufacturing of materials and technologies that may be poised to give Australia a competitive edge on a global scale (such as renewable energy opportunities and new battery technologies).

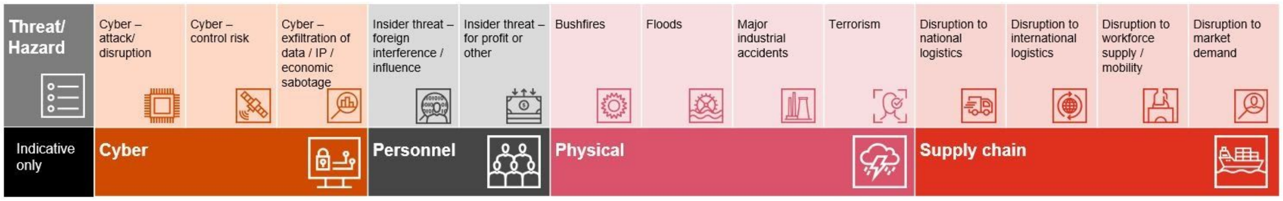
This view is informed by approaches adopted in other jurisdictions such as the United States, who in 2018 published a list of 35 mineral commodities that were considered ‘critical to the economic and national security of the United States’[1]. We would recommend similar analysis be conducted for Australia which would form valuable input into determining functions (such as mining, manufacturing and their supply chains) that are vital to our economy, security and sovereignty.

We would also suggest an explicit reference to ‘operational technologies’ in addition to ‘information technologies’ in the formal definition of critical infrastructure, which encompases the core systems many critical infrastructure operators rely on. Operational Technology, or OT, refers to systems that play a role in the control / coordination of physical devices and machinery, and includes technologies such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA).

From the perspective of impact, we believe there is an opportunity to reflect the future impact to our nation's prosperity and competitive advantage, as well as more immediate impacts that may be felt (which are already covered by the formal definition of critical infrastructure). For example, there may be elements of supply chains that are important for the development of emerging technologies, that if disrupted, may impact a future strategic advantage for Australia.

The below illustrates the type of threats and hazards incurred by many of the critical infrastructure operators we work with, across the four threat vectors outlined in the consultation paper.

Table 1. Threats and Hazards across vectors



Threat/ Hazard	Cyber – attack/ disruption	Cyber – control risk	Cyber – exfiltration of data / IP / economic sabotage	Insider threat – foreign interference / influence	Insider threat – for profit or other	Bushfires	Floods	Major industrial accidents	Terrorism	Disruption to national logistics	Disruption to international logistics	Disruption to workforce supply / mobility	Disruption to market demand
Indicative only	Cyber			Personnel		Physical				Supply chain			

The notion of ‘criticality’ is an important one, and needs to be assessed using a risk-based framework, with common language describing impact levels that are suitable from an all-hazards perspective. An example of this is the Criticality Assessment Tool (CAT) as part of the AESCSF, which seeks to stratify electricity providers based on inherent characteristics about their organisation and assets they own. Whilst part of a cyber framework, the CAT is not specific to cyber - these characteristics and the scoring method behind them remain valid regardless of a physical or digital disruption event.

[1] https://www.usgs.gov/news/interior-releases-2018-s-final-list-35-minerals-deemed-critical-us-national-security-and

There are a number of challenges in trying to derive such a criticality assessment across a broad range of industry sectors. One is data - ensuring you have enough data about critical infrastructure operators within an industry to be able to then stratify them across risk categories. For some industries this will be straightforward, whilst others may require more foundational work to understand current state and agree the common characteristics. The second challenge is then understanding how to categorise entities by risk, which may need to involve a combination of expert judgement, analysis of historic data, and simulation of potential future events (if / where historic data does not exist). Where there is a lack of data in trying to solve these problems, we would suggest starting with a simpler model that can then evolve over time.

The third challenge is granularity - whether to apply criticality at organisational levels, or asset levels, or some hybrid approach. This can lead to practical challenges in implementation, whereby for example, an organisation that is not considered critical but has 1 or 2 highly critical assets. Trying to adopt a ‘highest-common denominator’ approach may be impractical, but depending on various factors, may be the right approach especially in regards to cyber threats where the overall organisation is only as strong as its weakest point.

The assessment of criticality should ultimately drive the level of capability uplift / investment required by critical infrastructure operators. This may not be driven by the Positive Security Obligations, but the more detailed standards / requirements that sit under these (such as the criticality levels in the AESCSF).

Our view is that ‘Systems of National Significance’ should include entities whereby if disrupted or made unavailable, could directly and immediately cause harm to the health and safety of individuals and communities. By directly we mean without reliance on other entities / sectors, and by immediately we mean within minutes or hours. Within this category there may be a need for tiers of sub-criticality, i.e. impacts to large-scale metropolitan areas versus those to smaller regional communities. As an initial view, we would presume this to include some entities within energy, water and transport sectors.

Government-Critical Infrastructure collaboration to support uplift

Events of 2020 present a real opportunity for a step-change in the relationship between Australian governments and industry. We are seeing convergence of national security challenges and our social and economic prosperity as a nation. In our view, there is a window of opportunity to build on mutual recognition that successful recovery - and resilience to further shocks - will require close and trusted two-way engagement between government and industries critical to the provision of essential goods and services.

The TISN was the first step in opening the doors to Government and sharing (largely via a push model) with industry information on key risks and advice. This dynamic needs to mature to a two-way push-pull partnership that recognises there are volumes of essential data and modelling held by industry that together could dramatically improve real time situational awareness and drive better, collective decisions. Equally learnings from responses need to be shared openly and frankly to build resilience to future events.

A consistent risk lexicon will be key to translating engagement that was initially oriented around terrorism, to cyber and threats like bushfires and pandemics. There are different hazard indexes around the country for bushfires alone. Industry needs to be able to compare apples with apples to be empowered to prioritise and scale responses proportionately.

Similarly, advice needs to be simple and practical with tools and escalation channels for support - too often it is abstract, open to interpretation and difficult to justify the cost-benefit of investment. Information is distributed by an array of agencies at the federal and state levels increasing confusion and complexity. There is a significant opportunity to declutter this environment, make information more accessible, integrated and to better integrate behavioural insights into key messaging. This goes beyond critical infrastructure to engagement with broader business and communities and is an emerging theme from the NSW Independent Inquiry and Royal Commission into the Black Summer bushfires.

In terms of cross-sector dependencies, critical capabilities need to overlay geospatial dependencies as well as common nodes of operation. The Israel H-SOC, as described further on page 11, is an example of a facility built in collaboration with the Israel Government that achieves this level of situational awareness across critical infrastructure sectors.

Initiative 1: Positive Security Obligation

The principles proposed in the consultation paper are sufficiently broad in their coverage, but we would suggest some elements be explicitly called out in further detail. These include:

- Information sharing and communications, specifically for cyber security information and how that is collected, analysed and shared with relevant industry and government stakeholders
- Adherence to existing legislation / regulation, such as Australian Privacy Principles and the Notifiable Data Breach Scheme

We also believe there is an opportunity to more clearly show how these domains - cyber, physical, personnel and supply chain - are interrelated. There are natural synergies in these domains, such as the overlap of physical systems safety and cyber security for Operational Technology environments. Highlighting these links will help to avoid them being interpreted as silos and encourage buy-in, especially for sectors who have traditionally invested more in physical/supply chain risk rather than cyber.

Given the diversity of industry sectors under the new definition of critical infrastructure, we believe there is a good balance between clear expectations and tailoring to sector-specific needs. We would suggest, through this industry consultation, that the Department attempts to leverage some of the common language used by these sectors to make the requirements appear more relatable. For example, many industries would refer to the terms IT and OT rather than “ICT”, and the term “safety” is often used when discussing physical security (and is a core principle to many of these organisations) yet the word “safety” does not currently appear in these obligations

With respect to duplication with existing guidance and regulation, the Security Obligations and principles outlined in the paper on pages 19-20 appear to align to frameworks already used by many organisations either voluntarily or as a requirement for their sector. As a result, for those organisations in industries already seeking to align to these frameworks they will not require significant time and money to ensure they meet their obligations. Organisations with a low maturity level and no industry requirement for alignment may incur more significant costs to ensure they are able to meet their new obligations. This cost comes in the form of people (recruitment, training, cultural change), process (governance, policies, standard operating procedures) and technology (hardware, software, services).

From a people perspective organisations will need to increase the employment of individuals with the right skill sets, as well as ensuring organisation cultural uplift through educational and awareness programs. Throughout 2018, PwC’s Skills for Australia consulted widely across Australia to understand current and emerging developments in cyber security skills. Over 150 responses were received, representing 27 industries. The cross-industry, national project aimed to identify, develop and give access to common cyber training skills needs that can be used across a range of industries. PwC consulted nationally and found that stakeholders identified two key issues requiring urgent attention:

- A significant shortage of adequately trained cyber security individuals in the Australian workforce
- Lack of industry-aligned cyber security training
- People are also important through a strong organisational cyber culture in supporting their ability to meet these new obligations through a strong awareness and understanding of cyber threats and mitigations through education.

As examined in PwC’s Where Next for Skills, in the light of COVID-19 the impact of these key issues can be more keenly felt through the accelerated digitisation of many businesses[2].

Organisational uplift of capability for processes in order to meet these new obligations, would require both governance and oversight as well as maturing of existing processes and where required developing new ones. This would also be similar from a technology perspective requiring organisations to acquire new technical solutions and capabilities where there are gaps and maturing and developing existing solutions/capability.

[2] https://www.pwc.com.au/important-problems/where-next-for-skills/where-next-for-skills-report.pdf

Currently a number of sectors are subject to security obligations in-line with the principles outlined. For some industries this has meant they meet all the principles while others require enhancements. Some of the industries under current obligations and the focus of those obligations can be seen below:

Table 2. Current Regulatory Obligations

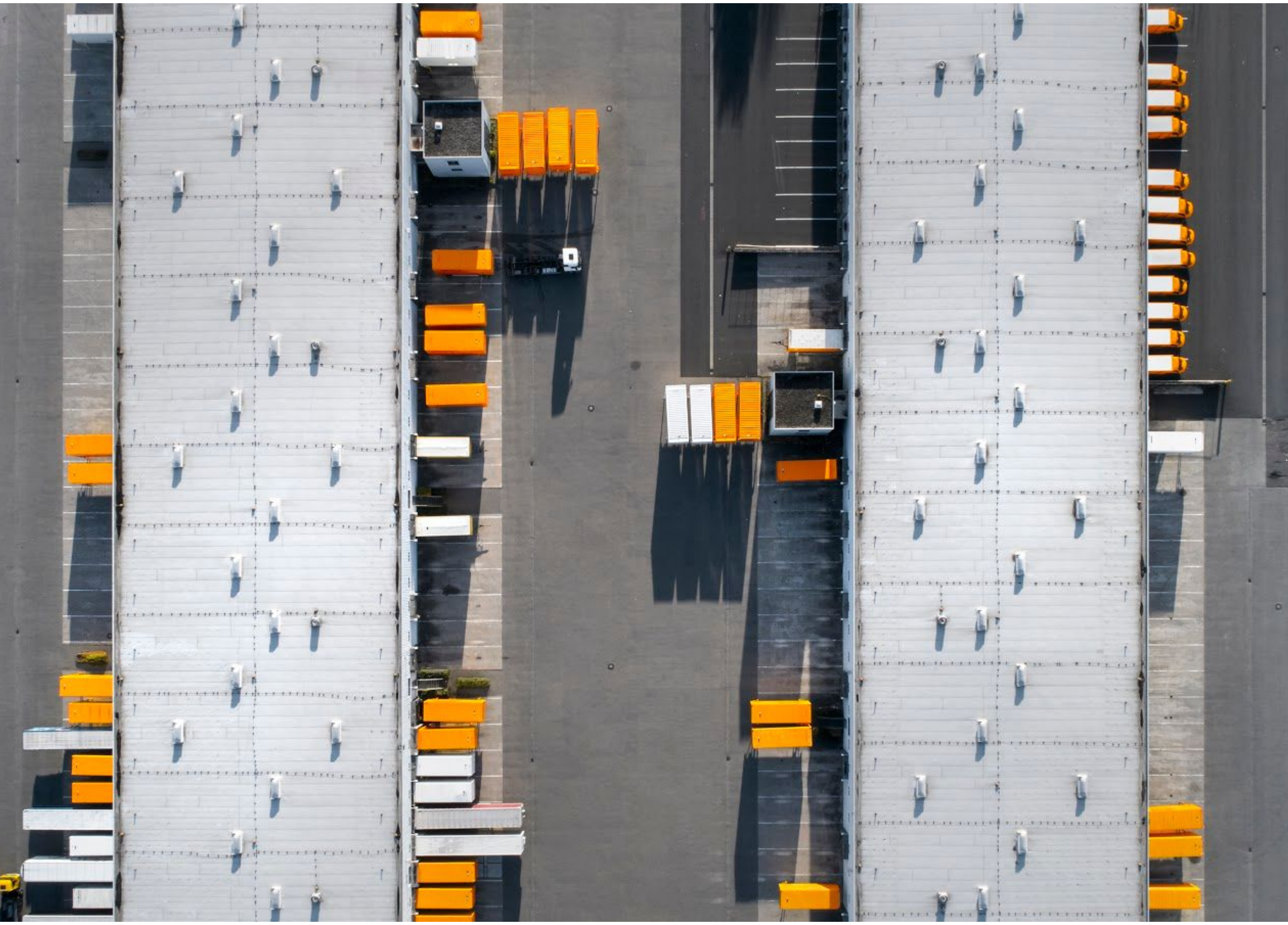
Name	Description
Australian Prudential Regulation Authority (APRA) APRA	For those organisations regulated under APRA there are standards in the form of the Prudential Standard CPS 243 Information Security laying out the roles required by the organisation, a baseline set of controls that should be inplace, the requirement of a Cyber capability that can manage the organisation effectively and notification requirements in the result of a Cyber incident.
Protective Security Policy Framework (PSPF)	As a Government policy, non-corporate Commonwealth entities must apply the The PSPF as it relates to their risk environment. It represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies. The PSPF is also considered better practice for state and territory agencies. This includes the controls put forward in the Information Security Manual (ISM).
Foreign Investment Review Board (FIRB)	FIRB through obligation requirements under the Foreign Acquisitions and Takeovers Regulation 2015 requires the declaration, and regular reporting for those organisations owned/purchased through a foreign investment approval ensuring a some level of oversight for supply chain security.
Security of Critical Infrastructure (SOCI) Act 2018	The SOCI Act 2018 currently ensures critical infrastructure organisations register and report on a regular basis to the CIC of Critical Infrastructure Assets as they are defined under the current definition of critical infrastructure.
Notifiable Data Breaches (NDB) scheme 2018	The NDB scheme 2018 for those organisations and agencies covered by the Privacy Act 1988 and the communication process and management of alerting individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach has occurred and is likely to result in serious harm to an individual whose personal information is involved.

Note: This list of regulatory obligations is not exhaustive and only covers high level examples of the regulation and obligations that Australian critical Infrastructure organisations may already need to meet. There are also considerations of state regulation and obligations and guidelines issued by industry bodies.

Given the broad nature of these PSOs, there will naturally be some duplication with existing oversight requirements and frameworks. The key is to ensure these requirements / frameworks are identified, understood and mapped in a way so that each industry sector can clearly understand the “hierarchy” of regulation and standards that is relevant to them. Extensive industry consultation is required here, but there is also a tremendous opportunity to drive a consistent approach on a broad cross-sector scale that has never been achieved before.

One of the key constraints across the Australian critical infrastructure landscape relates to skills within the Operational Technology (OT) and Industrial Control Systems (ICS) domain. These systems form the backbones of most critical infrastructure environments. The knowledge required to operate and maintain them is very specific. Throughout our work across multiple critical infrastructure sectors, we believe there is an opportunity for the government, in collaboration with specialist providers, to provide a baseline of skills through standardised training / education materials, that would greatly benefit the majority of critical infrastructure sectors.

As mentioned earlier in the paper, PwC played a key role in collaboration with AEMO, Home Affairs and ACSC in the development of the AESCSF. We believe it is achievable for the AESCSF to cover all-sectors as an ‘Australian Critical Infrastructure Cyber Security Framework’. This would result in a simpler outcome for Australian critical infrastructure operators, and importantly, a faster outcome, as the AESCSF is already well-embedded across the energy sector. In our recent experience, many organisations outside of the energy sector are already looking to the AESCSF as a fit-for-purpose cyber framework so we believe there is some appetite to pursue this approach. We also believe that the Criticality Assessment Tool (CAT) within the AESCSF could form the foundation of an all-hazards cross-sector criticality assessment methodology.



Initiative 2: Enhanced Cyber Security Obligations

To better protect our nation's critical infrastructure, the Government requires much closer partnerships with the relevant critical infrastructure owners/operators. This may entail the Government establishing agreements with operators, or via industry regulating bodies, that extend its reach into the private networks where these critical assets sit, for the purposes of detection and/or response capabilities. This interaction with private networks can take various shapes and forms - our suggestion is it should be a risk-based approach to provide cyber security intelligence sharing, detection and response capability for assets not only based on their criticality, but also their current level of cyber maturity. An example of such an initiative is the US Department of Energy’s Neighbourhood Keeper program, where they have partnered with Dragos to support the sharing of threat information to critical infrastructure providers, particularly the smaller and medium organisations who often lack their own cyber threat intelligence capability.

PwC believes the objective for the Government should be to support the establishment of cyber ‘situational awareness’ - in the form of technology, people and processes - across multiple critical infrastructure sectors, in collaboration with industry regulators, specialist vendors and critical infrastructure operators. In this context, ‘situational awareness’ refers to our ability as a nation, to maintain an up-to-date and holistic view of the cyber security threat and vulnerability landscape across critical infrastructure. We believe technology can play a key role in enabling the consultation, adoption and ongoing maintenance of critical infrastructure security reforms.

To maximise engagement with industry and the Government’s understanding of sector-specific issues, we recommend the Department and/or ACSC should commence a program of ‘reciprocal cyber resilience engagements’ with key providers of essential services across Australia. For example, a private sector organisation providing telecommunications services would invite a team of ACSC analysts onto their network to better understand how that infrastructure works and where vulnerabilities may exist. In parallel, cyber security staff from the telecommunications organisation would be invited to spend time at the ACSC to better understand how current and emerging vulnerabilities could be effectively addressed in their sector specific environment. We described this concept in our 2020 Cyber Strategy submission, and believe it is especially relevant given the broadening of the critical infrastructure definition outlined in the consultation paper.

The problem of how to rapidly declassify cyber threat intelligence for use by the private sector is a difficult one. There are real challenges to overcome: speed is critical for the intelligence to have value but going through a declassification process can take time. There are additional barriers where Australia is not the originator of classified cyber threat intelligence and it is received from partner countries at a given classification.

JCSCs have tried some workarounds to this problem, including offering to sponsor security clearances for some private sector JCSC partners. This approach has drawbacks - it is only limited to Australian citizens, and places the cleared individual in the difficult position of having to make decisions on what they can and can’t say or do with the information they learn, reducing the extent to which the intelligence is actionable. While challenging, rapid declassification of cyber threat intelligence is an important problem to solve, high-quality near-real time threat intelligence has the potential to increase the likelihood Australian businesses are able to detect advanced threats early.

It will be critical to look to other countries who have started this journey, a prime example being the National Hybrid Security Operations Centre (H-SOC) for Critical Infrastructure in Israel, which covers multiple industry sectors. The SOC provides visibility of over 200 critical infrastructure facilities across Israel, operating 24x7 in near real-time, connected directly to Operations and OT networks. The information gathered from these facilities is combined into a single "Big-Data Pool", with various external intelligence sources at all levels (public, national, municipal), analysed with the help of highly sophisticated algorithms, and supporting the detection and response capabilities for all facilities covered. PwC helped to design, develop, operationalise and manage this facility and there are a number of valuable lessons to be gained and shared from this.

Initiative 3: Cyber Assistance for Entities

There are situations in which the government should be able to take direct action to protect critical infrastructure, and in our experience many critical infrastructure operators would welcome this. Situations that are obvious candidates for direct government action include disruptive attacks by suspected state actors, or sophisticated intrusions that are beyond the capacity of entities to detect and respond to. Government could also play a role where an entity detects and responds to an incident by a sophisticated actor, but both Government and the entity are concerned about persistence (the actor remaining within the environment over a longer period of time).

Increased Government assistance is a net positive for critical infrastructure entities, but there are issues that could arise and require careful consideration. One issue is the potential imbalance between the security priority of the Government and the focus of private sector entities on maintaining operations / production. Situations could arise, whereby the risk appetite between Government and private sector entities differs substantially in relation to following a particular course of action.

Another issue that could arise is where directions are made with regards to Operational Technology (OT) environments. OT systems can be quite bespoke and there are a limited number of specialists within government with hands-on experience working in these environments. Obligations for these systems need to be closely co-developed with industry, and directions that relate to OT systems should generally be principle-based and receptive to feedback from entities to avoid adverse consequences. Interventions where direct action is taken should be carefully considered when OT systems are involved due to potential health, safety and environmental risks, and engineers from the entities should work alongside the Government to reduce the likelihood of adverse impacts when these intrusive powers are used.

We agree that the Government should have the capability to issue directions to critical infrastructure entities, consistent with the enforcement approach outlined in the consultation paper that sees these directives and interventions focused on entities that are deliberately non-compliant. We think some safeguards are important to underpin trust in the framework. There should be the capacity to appeal a direction, even if directions must be followed in the interim. This will provide an avenue for entities to contest directions that they believe are impractical, will weaken security, or have adverse impacts that may not have been fully considered.

The legal immunities for entities following Government directions flagged in the consultation paper are welcome. These protections are important because critical infrastructure entities typically have contracts with their customers, partners, and other entities that relate to their service obligations. Where obligations are breached because of a Government direction, it is appropriate that abeyance is provided from the consequences.

The consultation paper touches on the issue of disrupting perpetrators in exceptional circumstances and their location. Where perpetrators are located in Australia, we believe that existing Australian law (and cooperation with Australian telecommunications providers) provides sufficient mechanisms to respond to imminent threats or active incidents. In our view, more disruptive responses should be reserved for instances where the perpetrators are in a foreign jurisdiction that is uncooperative with the Australian Government's requests for assistance, or where the location of the perpetrators is unknown.

The costs of implementing these obligations will be substantial for many organisations that find themselves to be regulated by this framework. There may be substantial costs to uplift cyber security to meet the Positive Security Obligations, and among critical infrastructure entities our experience indicates there are those who have invested in cyber security and those that lag significantly behind. Government should not subsidise those entities that have not already made efforts to invest in a baseline cyber security capability. On the other hand, if the Government is seeking a new capability (e.g. technology to support a real time threat picture), or the obligations require a capability that goes beyond what enterprises should reasonably have established, then the Government should fund that capability in the public interest.

Lastly, we encourage the Government to set the right tone when they launch the new reforms, with an emphasis on the responsibility that all critical infrastructure entities have for their own cyber security. There is no doubt that some who welcome an increased Government role in protecting critical infrastructure do so because they see cyber as a complex and substantial risk, and an increased government role as transferring or co-owning the risks.

Like any organisation exercising appropriate risk management, critical infrastructure entities should have their own capability to detect and respond to cyber security threats, and shouldn't be reliant on the Government to respond on their behalf. It must be made clear to these entities that the Government only has limited capacity to respond and will only do so in specific circumstances in the interest of protecting our nation and its citizens.