Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

CISCO AUSTRALIA RESPONSE TO THE PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFCANCE CONSULTATION PAPER 2020.

Cisco welcomes the opportunity to respond to the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper 2020.*

Our submission to *Australia's Cyber Security Strategy 2020* stated Cisco's support for the government's initiatives to bolster Australia's overall security. This support is built on Cisco's commitment stated in our *Country Impact Plan* to help sustainably grow and protect the Australian economy, communities, businesses and organisations. We appreciate the opportunity to constructively contribute to this consultation process.

In today's connected world, everyone benefits from advanced cyber defence programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations, especially during the time of a pandemic, is essential to keeping our society functioning.

Cisco acts both as an operator of technology equipment and services used in industries deemed critical (e.g. Telehealth) as well as a supplier of equipment and integration services to these industries. The security of our customers' endpoints, networks, programs and data is paramount to Cisco and our comments to this consultation are made with our customers' interests in mind, both public and private sector.

We also consult with government and industry organisations globally about critical infrastructure technologies and protection and bring that perspective as well as local expertise to this debate.

Cisco staff have participated in many of the workshops across the various industry groups and sectors and we wish to congratulate the Department of Home Affairs and federal government for the direct and open consultative engagement with stakeholders.

Our response to the consultation paper in summary is:

- The overall focus on uplifting the security of critical infrastructure and national systems of significance is important policy work and should continue to be undertaken carefully, methodically and without haste to maintain strong industry support and collaboration;
- Uplifting cyber security for businesses, organisations and government agencies should focus on improvements across all sectors, not just the top two tiers (ie, not just Regulated Critical Infrastructure Entities and Systems of National Significance);
- The proposed initiatives and $68m government investment in intelligence sharing platforms, new JCSC community liaison officers and proposed amendments to TISN are welcome, but the objective of better intelligence sharing arrangements has been difficult

to achieve in practice and this requires particular attention in order to make meaningful progress;

- The focus of *Australia's Cyber Security Strategy 2020* on supply chain security is essential and Cisco welcomes the commitment from the government for improved two-way information sharing through the ACSC's new platforms, and improved threat intelligence and situational awareness capabilities;
- The federal government's commitment and funding to uplift its cyber security defence capability and to act as an exemplar for the rest of the economy is important to the overall success of *Australia's Cyber Security Strategy 2020*, a point made at 'objective 4' *Australia's Cyber Security Strategy 2020: industry advisory panel report*;
- Properly resourcing all federal government agencies to meet their cyber security obligations and ensuring transparent reporting of progress will act as an incentive to businesses and organisations to also meet their obligations and raise the overall uplift of cyber security across the economy;
- Capabilities, lessons and best practices ought be shared across the Australian Public Service and through consultations with state, territory and local governments and public service commissions;
- Regarding costs, businesses and organisations required to meet additional security standards as a result of this policy may seek to pass these costs on to consumers. Cisco customers are already heavily invested in security capabilities and services and ought not be required to incur additional significant costs where these are not proportional to the risks attached to their operations. Should the government determine that a business or organisation is part of an SNS or RCIE and could be linked to systemic security issues, government should consider how additional security obligations that may be required to meet system wide threat concerns or standards are funded;
- Existing security regulatory arrangements and existing regulators must be thoroughly examined, and any gaps publicly reviewed, prior to the creation of new regulations or regulators. Duplication must be avoided at all costs, which has been the commitment given during the consultation process to date. The additional costs of establishing new regulators or enabling security functions within existing regulators could be high;
- Data and Cloud is a regulated industry that operates horizontally across all industry verticals and is already subject to national and international standards and regulations. It should not be subject to a specific cloud regulator that would duplicate the functions of existing arrangements and needlessly increase costs. Cisco can provide information to the proposed sector based workshops to inform views about appropriately tailored security for cloud and data services across each industry vertical;

- The definition of a business or organisation as CIE, an RCIE or an SNS will have an impact on the operation of the business. There should be an appropriate process for a business or organisation to appeal the definition it is allocated at any time. The regulator may be the best entity to define the category of a business to ensure a flexible approach;
- There must be checks and balances for all government assistance and especially step-in powers. Without a defined operating model on how the step in process would work, it is difficult to determine the checks and balances required but there are examples provided in other parliamentary reviews into security laws that could provide guidance;
- It is not clear yet what impact the government assistance powers to step-in could have on the operation of companies that are either not headquartered in Australia or operate in off-shore markets. For example, Cisco provides standardised equipment and services across the globe and does not modify equipment or services.
- Similarly, in the multi-tenant public cloud model common across IaaS, PaaS, and SaaS cloud providers, the relevant operations and security teams not only protect CIE, RCIE, and SNS entities but also other Australian and overseas organisations. Step-in powers in such an environment needs to be cognisant of the concerns, rights and legal arrangements of unrelated entities globally.

Further detailed comments addressing the consultation paper questions:

The expansion of the industry sectors to cover a more holistic range across Australia is consistent with current approaches in other parts of the world. Governments should undertake regular reviews across industry sectors and even specific companies that could be deemed critical to the health of the economy and society, and could be targeted for cyber attack . This could be especially the case in a post pandemic economy where market leading industry players may emerge and grow quickly to become important to the systemic operation of the economy.

The three-tier enhanced regulatory framework model for defining critical infrastructure and systems of national significance allows security obligations to be right-sized for the size and economic reach of the entity. Cyber security uplift across the entire sector should remain the goal, and not just focus on the more significant tiers.

Protecting SMBs

Cisco welcomes the focus of *Australia's Cyber Security Strategy 2020* and the *Protecting Critical Infrastructure and Systems of National Significance consultation paper 2020* on seeking ideas on how best to protect smaller and medium sized businesses from cyber security threats.

The government's investments in intelligence sharing, skills and workforce development and a focus on 'cleaner pipes', among other initiatives, will assist to better protect SMBs.

Further initiatives could include working with companies and organisations that supply important services to SMBs, such as banks, internet service providers, accounting and tax providers and peak industry bodies to provide bundled, accredited and authorised cyber security products and services to their customers or members.

Telecommunications companies and internet service providers are already providing these products and services and have specialist knowledge and quality control capabilities.

An example of an industry partnership to better protect SMBs is Cisco, the National Australia Bank (nab) and Cisco partner, Outcomex, to provide a wholistic cyber security service through a Cisco security product, Umbrella. This includes preferential pricing for nab customers and recognises nab's investment in the security of their customers' businesses and also represents an investment by nab into the overall health of SMB security across the economy. Further information on this partnership can be found at: https://www.nab.com.au/business/small-business/moments/manage/planning/cyber-security-software and Cisco Umbrella information is here: https://www.nab.com.au/about-us/security/business-safety-tips/cyber-threats-business-protection

Cisco has also partnered with the Council of Small Business Organisations of Australia (COSBOA) to provide information to COSBOA members about the importance of appropriately protecting their businesses and the steps they can take to improve their cyber security posture.

Other organisations where SMBs receive business critical services such as accounting businesses and peak bodies, industrial relations bodies and tax advisers could also be supported to provide accredited, bundled products and services to their members.

With the proposed expansion of the number of sectors, the concept of critical "infrastructure" is also being applied to critical "services." "Systems" of National Significance is inclusive of both. The term Essential Service Providers is already widely used and covers organisations whose impact is far more localised. Hence, "Critical Infrastructure and Services" is suggested as a more suitable revised term for the expanded scope of the Act.

Many sectors have interdependencies on each other, particularly when viewed through the lens of coordinated attack. Water services near a military base, power for a regional data centre, and transportation for food and grocery are all very evident examples. For Data and Cloud, the interdependency is extreme. Within the sector, there is potentially SaaS dependent on PaaS dependent on IaaS dependent on DCaaS, often across multiple vendors and jurisdictions. Cross-sectorally, any CI sector may depend on any variant of XaaS and do so with no commonality to the dependency of a peer organisation in that same sector. As such, it may be difficult to define Data and Cloud as a "standard" Critical Infrastructure domain, particularly regarding operational aspects of reporting incidents. It may be easier to capture this domain through dependency mapping within other domains, which would be important across all sectors and entities. Existing Data and Cloud provider intrinsic capabilities that provide High Availability, Disaster Recovery, and Business Continuity are already eligibility criteria to provide services to not only CI but cloud tenants generally. With respect to CIE, RCIE, and SNS dependency on Data and Cloud providers, newly added sectors and regulators should look to the existing approach used by telecommunications and banking sectors for guidance.

Treatment of Data and Cloud as a “horizontal sector”

From a Critical Infrastructure and Systems of National Significance viewpoint, the criticality of Data and Cloud services is generally “inherited” from the criticality of their customers business functions that are data or cloud dependent. It may be challenging to apply the “all hazards” concerns of the proposed framework to data and cloud providers independent from the context of their CI sector customers. Such may be the variety of concerns that they may be difficult to consolidate for any potential Data and Cloud sector regulator to apply.

Rather than a Data and Cloud sector specific regulator, providers should be required to meet the appropriate per sector regulatory requirements of their customers.

However, it is important for providers to have engagement in the development of any per sector security guidance. Data and Cloud providers already have a strong commitment to international standards for security and risk management.

A core principle in development of the new framework should be to default to a recognition of existing standards and assessments already held by Data and Cloud providers such as:

- AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security, management systems—Requirements
- and, AS ISO/IEC 27002:2015 Information technology - Security techniques - Code of practice for information security controls

Note: These are already recommended standards within the current *Telecommunications Sector Security Reforms* (TSSR).

Additionally, this principle should extend to the recognition of independent assessments and audits of security controls such as System and Organisational Controls (SOC) defined by the American Institute of Certified Public Accountants.

Whilst not an exhaustive list of potential standards to recognise (a list should be developed in conjunction with industry), it would avoid significant costs on providers and ultimately their customers. A lack of alignment and commonality of approach between potentially 10 sector regulators could see providers in Australia face a multitude of differing assessment programs similar to the public sector IRAP/ISM based cloud assessments.

Threats across this entire domain are evolving rapidly, and the type of attacks across all these sectors can be complex, targeted, multi-staged attacks or non-targeted relatively simple attacks. As an example, whether malware which encrypts data was delivered to an organisation via complex targeted attack or a non-targeted email phish, the impact to the organisation can be the same. Hence, even in the absence of a current sector specific threat all organisation should aim to continuously uplift their cyber posture. This is where there is an intersection of the goals of both this critical infrastructure review and other initiatives of the Cyber Security Strategy 2020. Attacks can target supply chains as a way of gaining a foothold to their ultimate targets, making it difficult to categorise and right size industries for inclusion in the framework. The goal should be uplift across entire sectors while simplifying the engagement model for smaller operators, as opposed to trying to capture all in a higher level definition. The detailed work of regulators through industry specific consultations will be important to achieve this goal.

With sophisticated and complex cyber threats, simple disaggregation of critical services should not be considered as mitigation or protection. Smaller businesses and organisations, generally, tend to have less mature capabilities not only due to the complexity of cyber security and the cost of access to sufficient in-house expertise, but also as their maturity level is appropriate for the needs of their organisation. However, sufficient compromise and attacks on smaller players can aggregate to significant risks. Hence, enhanced focus on assistance for smaller entities to uplift cybersecurity could represent an increase in overall resilience across the sector – even those which fall below the threshold of a Critical Infrastructure Entity. Government Assistance such as an enhanced TISN program should also encompass the whole of economy tier. A threshold based approach for defining which tier an entity may be in is not the best way of doing things. Leaving the categorisation up to regulators may be more agile and effective, also giving entities a simple and inexpensive mechanism for appeal.

The focus on entities as the legal construct for ownership and operators for this legislation is understandably necessary. A question has to be asked what actions are going to be legislated should the entities ownership or operation be deemed a risk? For example, looking at this through the lens of virtual assets such as licensing of intellectual property and technology held by companies, these could be created sufficiently small as to escape higher regulation. It is important that explicit powers, their usage, and processes involved are called out within legislation to enable business to make informed investment decisions.

The definition of systems of national significance should be based on dependency mapping and supply chain data and analysis to indicate any potential entities with a high amount of dependency. When it comes to defining the tiers of critical entities, whilst disaggregation is a mitigation, it is not absolute protection. In some cases, isolated incidents are significant in terms of social impact. An example of this is if a cyber attack resulted in a casualty at a hospital, the loss of trust could sufficiently disturb the entire healthcare system. The Data and Cloud sector, for example, has many cross-industry interdependencies and representation from these sectors should be included in sector workshops as further details are worked through.

Regulators and industry bodies informing classification of entities under the framework should include clear lines of accountability. The proposed model takes an all hazards approach, including cyber security. The Singapore model is worth examining, whereby the Cyber Security

Agency (ASD equivalent) works with industry regulators that have responsibility across the industry, in order to define the cyber security requirements for those industries.

Cyber regulations need experts from the industries and broader cyber security experts in order to inform the controls and capabilities. The TISNs could effectively act in a greater capacity with additional expertise being invited in to participate from outside the regulated sector, where necessary. This is important in order to have a diverse perspective and such cybersecurity skill sets are not commonly found particularly in operational technologies.

The Data and Cloud TISN would also act cross-sectorally, ensuring commonalities are leveraged. Leveraging existing standards and practices, where appropriate, lowers the costs involved and ensures coordination across sectors that would have the same advantage. This approach also allows input from experts outside of specific sectors. Historically, the TISN's have not been open to membership from outside of the sector or government. The representation of data, cloud and communications industries is important particularly for cyber security.

Cross sector dependencies are potentially better represented through considering supply chain dependencies. These dependencies need to be identified through an operator-by-operator basis, and have appropriate controls, guidance, and contractual obligations for all dependencies identified as necessary to meet the critical obligations of the operator.

Rationalisation of risks should happen at a level greater than an individual entity, with the perspective of the infrastructure being critical to other entities or the nation. Risks should be evaluated through the lens of the inter-dependency mapping.

All security comes with cost, and it is welcome that government is investing to centralise some aspects and providing tools and processes to assist. Care should be taken to avoid unnecessary certifications, as bespoke certifications are very costly to initiate and maintain. A centrally managed list of vetted vendors could be useful to simplify vetting when it comes to supply chain requirements for critical infrastructure, for example. Providing toolsets for asset vulnerability, risk reporting, and even internet facing and cloud security capabilities, could potentially be centralised, which can enable focus on other areas for entities, but also ensure adequate coverage across the critical sectors for capabilities.

Cisco is committed to internationally and widely recognised standards including Common Criteria, ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, SOC2 as certifications and audits for our products. This is a good place to start for certification requirements. These certifications are multi-domain certifications and cover personnel, physical and operation security as well.

Incident reporting should be clearly defined. The definition of an 'incident' and reporting obligations can quickly become unmanageable if this is too broad. Incidents can be un-investigated, investigated and deemed false positives, investigated, and deemed non-impactful or deemed a breach. An understaffed entity may have a lot more incidents in the first category than a well funded one. The level of detail of the incidents that needs to be shared may also be difficult to define. All of these factors become difficult when looking at incident sharing mechanisms in real time.

A Security Incident for Cisco is where an adverse event has happened that threatens or compromises the confidentiality, integrity, and availability of Cisco's infrastructure, data or information assets. These are managed via a ticket within a security management platform, that begins with an event of significance that has occurred and warrants further investigation. Information from various systems and sources of information (e.g. internal emails) are normally appended to these incident cases and are often very sensitive in nature. Classifications such as severity of an incident may change depending on the perceived potential impact throughout the investigation.

Cisco practises the highest level of integrity and maintains as much transparency as possible when it comes to sharing Security best practices, especially with aligned governments and such trusted customers and partners. As security practitioners, we share incident stories wherever possible that have demonstrable learning and that could be adapted by others, after going through sanitisation for customer and Cisco confidential data. We also share threat intelligence through advisories with our trusted customers and partners, which is a more dynamic endeavour achieved through the efforts of our Cisco Talos Research group.

Cisco actively forms relationship for threat intelligence, globally, through our intelligence arm Talos. Talos are a world leader in threat intelligence. Talos maintain threat sharing relationships with ISACs and National CERTS – in Australia this is with the Australian Cyber Security Centre (ACSC) and we are supportive of extending this to the Joint Cyber Security Centres (JCSC) as part of the expanded threat sharing platform announced in the Cyber Security Strategy 2020. This is an area for opportunity for increased efficacy with a push toward current threat information sharing. We are supportive of efforts to deliver a new threat sharing platform providing the capability for more real-time, bi-directional sharing of threat information from a multitude of sources.

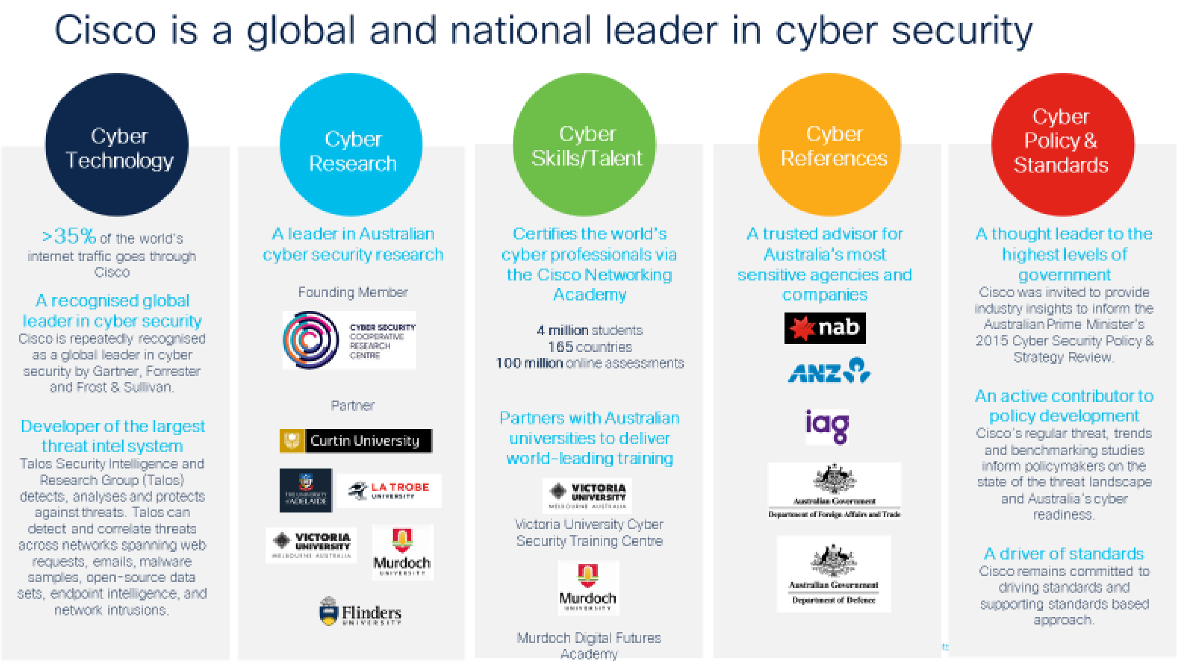
It is important in reviewing the role of the TISNs, the JCSCs and the new threat sharing platform that government is mindful that the information is *actionable*. Across sectors, there will be a range of maturity and capability to act on any information shared. In some sectors, the desired outcome (protection) might be better achieved by sharing threat information with security solution vendors and managed security providers. This highlights the value of including organisations nominally thought as being outside of a sector into the conversation.

The ability for a government to step in times of national disaster or last resort should have appropriate checks and balances. Such actions may only be necessary if the entity is incapable, unresponsive, or openly hostile. The regulator should be part of the decision making process and it should be informed by experts.

Clarity is required on how other related initiatives in *Australia's Cyber Security Strategy 2020* relate to the security of CI, RCI, and SNS to avoid per sector duplication. Protective DNS (pDNS) is an existing ACSC initiative provided to government and select CI providers. Also mentioned in the strategy is Telstra's Cleaner Pipes initiative. Additionally, there are commercial cloud providers of protective DNS services. As a fundamental technology of the Internet, will the provision of such services be deemed a CI service or only if that service is delivered to a CI entity? In that scenario, is the ACSC itself a CIE, RCIE, or SONS as the provider of pDNS service to government and CI?

Cisco is supportive of initiatives to provide relatively easy to deploy solutions such as protective DNS to all sectors of Australia (ideally the entire country), and we see this and similar initiatives as important parts of uplifting cyber security posture. Of course availability considerations must be included as well as mobile asset and automated protections. These types of efforts can be funded centrally by government, gaining economies of scale and alleviating the cost burden to business.

Cisco appreciated the consultative approach, is supportive of the steps the Australian government seeks to take and would like to remain engaged as the next steps are taken. Whilst it is always a good time to increase the cybersecurity and preparedness of critical infrastructure, this effort does feel hurried and the aggressive timeline ambitious.



Cisco is a global and national leader in cyber security

Cyber Technology

>35% of the world's internet traffic goes through Cisco

A recognised global leader in cyber security
Cisco is repeatedly recognised as a global leader in cyber security by Gartner, Forrester and Frost & Sullivan.

Developer of the largest threat intel system
Talos Security Intelligence and Research Group (Talos) detects, analyses and protects against threats. Talos can detect and correlate threats across networks spanning web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions.

Cyber Research

A leader in Australian cyber security research

Founding Member

Partner

Cyber Skills/Talent

Certifies the world's cyber professionals via the Cisco Networking Academy

4 million students
165 countries
100 million online assessments

Partners with Australian universities to deliver world-leading training

Victoria University Cyber Security Training Centre

Murdoch Digital Futures Academy

Cyber References

A trusted advisor for Australia's most sensitive agencies and companies

Cyber Policy & Standards

A thought leader to the highest levels of government
Cisco was invited to provide industry insights to inform the Australian Prime Minister's 2015 Cyber Security Policy & Strategy Review.

An active contributor to policy development
Cisco's regular threat, trends and benchmarking studies inform policymakers on the state of the threat landscape and Australia's cyber readiness.

A driver of standards
Cisco remains committed to driving standards and supporting standards based approach.

CYBER SECURITY COOPERATIVE RESEARCH CENTRE
Curtin University
THE UNIVERSITY of ADELAIDE
LA TROBE UNIVERSITY
VICTORIA UNIVERSITY MELBOURNE AUSTRALIA
Murdoch UNIVERSITY
Flinders UNIVERSITY
VICTORIA UNIVERSITY MELBOURNE AUSTRALIA
Murdoch UNIVERSITY
nab
ANZ
iag
Australian Government Department of Foreign Affairs and Trade
Australian Government Department of Defence