NORTHROP GRUMMAN

SUBMISSION

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

16 September 2020

CONTENTS

INTRODUCTION

Northrop Grumman Australia welcomes the opportunity to make a submission in response to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (the Consultation Paper).

While the threat of cyber attacks from state and non-state actors is ever-present – as the ongoing attacks on Australian government and critical infrastructure networks has demonstrated – coronavirus has provided an opportunity for such actors to step up their activities to an unprecedented level, both in terms of effort and sophistication.

The heightened level of malicious cyber activity carried out under the cover of coronavirus has coincided with an increased level of vulnerability as businesses moved en-masse to remote working. Australians rely on critical infrastructure and connected technologies for all facets of their lives and every Australian business relies on these sectors to secure its prosperity and the growth of the national economy. In order to safeguard this prosperity, Northrop Grumman Australia welcomes the government's rethinking of Australia's cyber security policy. It is important that as the government expands the critical infrastructure regulatory framework, it focuses its objectives on building national resilience and greater cooperation between the public and private sectors; in particular, ensuring the cyber-worthiness of critical public infrastructure entities.

The Consultation Paper poses 36 questions in its "Call for views" from critical infrastructure industries. As a global leader in high-end critical cyber incident response, a defence industry sector representative, and a provider of sovereign Australian developed cyber technologies, Northrop Grumman Australia will focus our submission on a selected number of those questions, where we can best leverage our expertise as a trusted cyber partner and advisor to government and critical infrastructure entities to provide relevant insights.

In this context, Northrop Grumman Australia would like to commend the federal government on the release of the 2020 Cyber Security Strategy and the work it is undertaking to ensure Australia's security practices, policies and legislation enhance the security and resilience of Australia's critical infrastructure.

RECOMMENDATIONS

Northrop Grumman Australia recommends that the Department of Home Affairs and the Australian Government consider the following recommendations:

1. The Australian government should restructure the proposed classification levels as clearly defined tiers: Tier 1 – Systems of national significance; Tier 2 – Regulated critical infrastructure entities; Tier 3 – Critical infrastructure entities; and Tier 4 – Whole of economy.
2. The Australian government should codify Australia's defence industry as regulated critical infrastructure.
3. The Australian government should be enabled, through the *Security of Critical Infrastructure Act 2018,* to flexibly designate (permanently or temporarily) specific defence industry critical infrastructure entities as a higher 'entity level' classification than the wider sector.
4. The Australian government should expand the list of critical infrastructure sectors under the proposed legislative reform process to include meteorology, and consider the addition of other relevant public service entities.
5. The Australian government should work with industry to design, develop and implement the collaborative critical infrastructure activities identified in the Consultation Paper to support cyber resilience uplift.
6. The Australian Cyber Security Centre should establish and coordinate 'on-call' joint public-private teams to respond rapidly to advanced persistent threats and large-scale cyber attacks on critical infrastructure entities.
7. The Australian government should consider opportunities to support and partner with industry to develop and deliver cyber education initiatives to attract the next generation of cyber professionals.
8. The Protective Security Policy Framework (PSPF) and the related Information Security Manual (ISM) sets out the requirements for protective security to ensure the secure continuous delivery of government business. The PSPF and ISM also apply to industry providing goods and services for government departments and agencies. If the PSPF and ISM represent Government's best practice then it should be used to provide guidance for CI and SONS.
9. The Australian government should work with cyber industry experts to develop a risk framework, and corresponding maturity framework, to assess the cyber preparedness of critical infrastructure sectors and ensure the consistent application of Positive Security Obligations across the various sectors.
10. The Australian government should develop and implement a comprehensive engagement strategy targeted at critical infrastructure sectors and entities to enhance cyber awareness and culture and encourage them to implement strong security awareness practices and protocols across their organisations.
11. Critical infrastructure entities subject to Positive Security Obligations should be required to examine their baseline level of security and conduct regular health checks to ensure an appropriate level of maturity is in place.
12. The Australian government should appoint critical infrastructure cyber security sector regulators, with a clearly defined role and remit. Regulators should be encouraged to establish strategic partnerships with industry, to support the development, delivery, assessment and ongoing regulation of the Positive Security Obligations for each sector.
13. The Australian government should implement a "systems architect" to oversee the regulation of the entire critical infrastructure system and enforce a common set of standards for critical infrastructure security.

14. The Australian government should mandate the reporting of cyber incidences to entities categorised as ‘systems of national significance’ and encourage voluntary information-sharing by all critical infrastructure entities to support the development of a national threat picture.
15. The Australian government should work with industry to de-stigmatise cyber incident reporting.
16. The Australian government should encourage all critical infrastructure entities to participate in a voluntary framework of enhanced cyber security obligations, beyond those designated as ‘systems of national significance’.
17. The Australian government, Department of Home Affairs and Australian Cyber Security Centre should engage strategic industry partners with experience and expertise in managing the entire spectrum of cyber intrusions through to critical incident response, to ensure cyber playbooks are fit for purpose.
18. The Australian government, Department of Home Affairs and Australian Cyber Security Centre should engage expert industry partners to assist in delivering strong, decisive cyber effects in the event of a cyber intrusion on an Australian critical infrastructure entity.

NORTHROP GRUMMAN AUSTRALIA'S CYBER EXPERTISE

Northrop Grumman Australia is a wholly owned subsidiary of the Northrop Grumman Corporation, a global leader in space, aeronautics, defence and cyberspace. Through science, technology and engineering, our 90,000 employees create and deliver advanced systems, products and services to meet the ever-evolving needs of our customers worldwide.

Northrop Grumman Australia works with the Australian government to deliver world-class capability in support of Australia's defence, security and national interests. The company is extremely proud of our mature relationship with the Commonwealth of Australia and is committed to enhancing our business and geographic footprint in Australia. Northrop Grumman Australia has a strong customer base in Australia and has been supporting a variety of defence and civil programs in the country for more than 20 years.

Northrop Grumman Australia is a global leader in high-end cyber and critical incident response, and a trusted security partner to many of our government and commercial sector customers. We have a local C5 (command, control, communications, computers and cyber) business unit that boasts an experienced Australian cyber workforce. We are also currently prototyping an Australian innovation that secures communication endpoints (legacy and internet of things), even in the event of the underlying network being compromised. However, our real value-add to Australia's national cyber resilience goes beyond our products and is highlighted by our proactive partnerships with government and critical services.

We offer end-to-end development, deployment and integration of cyber security capabilities that encompass active cyber defence and resilience; full-spectrum operations; intelligence and information management; and information and computer technology (ICT) and network security. We deliver trusted cyber and intelligence services to a range of government, commercial and non-profit clients including architecture design, software engineering and configuration, security accreditation and assessment, and cyber training. Our services are complemented by a range of high-quality, locally designed and developed cross-domain cyber product solutions to rapidly elevate enterprise security among Australian businesses and critical infrastructure entities.

As an experienced global leader in cyber capabilities, Northrop Grumman Australia has partnered with state and federal governments to support the development of a number of government cyber policies and frameworks. Northrop Grumman Australia's Chief Executive, Chris Deeble, was a member of the Minister for Home Affairs' Industry Advice Panel, which provided strategic advice and guidance on the development of *Australia's Cyber Security Strategy 2020* (the 2020 Cyber Strategy). The company is also represented on the NSW Cyber Security Standards Harmonisation Taskforce.

CASE STUDY: AUSTRALIAN NATIONAL UNIVERSITY

In early November 2018, a sophisticated actor gained unauthorised access to the network of the Australian National University (ANU), a major tertiary institution in the national capital, with links to government and security agencies.

The attack breached part of the network housing the university's human resources, financial management, student administration and enterprise e-forms systems, with the actor able to copy and steal an unknown quantity of data contained in those systems.

The early stages of the attack relied on an email containing malicious code being sent to a senior member of staff. This email was "interaction-less", meaning it did not need to be opened in order to activate the malicious code, which sent the senior staff member's credentials to several external web addresses. The report into the attack notes "it is highly likely that the credentials taken from this account were used to gain access to other systems".

Once these systems were compromised, the actor was able to launch further attacks from within the system itself, bypassing external protective measures and making them redundant in this case. Detection of the actor's presence precipitated an incident response, led by Northrop Grumman Australia, working with the ANU cybersecurity staff. The ANU has now considerably increased its technical cybersecurity efforts, with the support of Northrop Grumman Australia. The investigation following the breach was conducted in close cooperation with Australian government security agencies and Northrop Grumman Australia.

The ANU, in partnership with Northrop Grumman Australia, is now undertaking the development of a strategic information security program, which encompasses the modernisation of information technology and security infrastructure, coupled with a strong focus on growing a cyber-aware culture. The partnership will provide the opportunity for the ANU to leverage the experience and insight from Northrop Grumman Australia cyber specialists to grow the knowledge and experience of staff and students coming through the university.

DEFINING AND CATEGORISING CRITICAL INFRASTRUCTURE ENTITIES

The 2020 Cyber Strategy notes that around 35 per cent of cyber incidents impacted critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy. This was reinforced in Prime Minister Scott Morrison's 19 June 2020 announcement[1] that Australian organisations were being targeted by a sophisticated, state-based actor.

The key message is that such attacks are occurring with greater frequency and are unlikely to be directed towards "hard" assets such as defence or security agencies. Rather, they will likely target critical infrastructure such as power grids or hospitals, which may not be as well secured, but the disruption of which would be devastating for the community and the economy.

The security of Australia's critical infrastructure can best be described as a "system-of-systems", with discrete systems joining together to form an interdependent whole, in much the same way that individual bricks build an entire wall.

In order to enable a more secure online world for Australians, their businesses and the essential services upon which they depend, the 2020 Cyber Strategy notes that this critical infrastructure needs to be protected from the most sophisticated of threats.

As noted in the Consultation Paper, the first step in protecting critical infrastructure is defining what it is. The Department of Home Affairs' Critical Infrastructure Centre notes that Commonwealth, state and territory governments currently define critical infrastructure as:

> *"Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."*[2]

The proposed classification scheme spanning whole of economy, critical infrastructure entities, regulated critical infrastructure entities, and systems of national significance is difficult to understand. Northrop Grumman Australia recommends that the Australian government apply a simplified tiering system, overlayed with the proposed classifications, which will assist critical infrastructure entities in determining where they sit within Australia's national resilience, as they seek to develop their local capabilities.

Recommendation 1: The Australian government should restructure the proposed classification levels as clearly defined tiers:
Tier 1 – Systems of national significance;
Tier 2 – Regulated critical infrastructure entities;
Tier 3 – Critical infrastructure entities; and
Tier 4 – Whole of economy.

[1] "Statement On Malicious Cyber Activity Against Australian Networks" (19 June 2020) retrieved from https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks
[2] "Safeguarding Critical Infrastructure", Critical Infrastructure Centre, retrieved from https://cicentre.gov.au/infrastructure

CATEGORISATION OF DEFENCE INDUSTRY

Australia’s defence industry plays a crucial role strategically, domestically and economically. It is essential to the Australian Defence Force’s (ADF) ability to protect the country’s interests and provides the sovereign capability that allows the ADF to act with greater independence in an increasingly contested strategic environment.

In addition to its role in the Indo-Pacific, the ADF has also been called upon to help Australian citizens at home, evacuating them during the 2019-20 bushfire season, and assisting with the government’s health response to the coronavirus pandemic. Throughout these missions, the ADF has been supported by Australia’s defence industry, whether that be contractors helping get *HMAS Adelaide* to sea in less than 48 hours to rescue stranded families, or assisting in the manufacture of personal protective equipment and ventilators amid coronavirus.

Australia’s defence industry has also shown its economic value during the coronavirus pandemic and resulting economic recession. This has been demonstrated by defence industry’s ability to keep its doors open and workers employed in a vital contribution to the federal government’s economic response to the pandemic.

Given the central role Australia’s defence industry plays in enabling the ADF’s international and domestic activities, it is appropriate that it be formally codified in the government’s legislative definition of critical infrastructure under the *Security of Critical Infrastructure Act 2018*. Northrop Grumman Australia supports the definition of defence industry critical infrastructure, as proposed by the Department of Home Affairs during the virtual ‘Defence Industry Workshops – Protection of Critical Infrastructure and Systems of National Significance’ consultation session hosted on 7 September 2020. Under this definition, critical infrastructure defence industry assets are:

> *Those assets that provide a critical capability, or supply, sustain or enable such a critical capability, for Defence. A critical capability includes material, technology, platforms, networks, systems and services that is required for Defence to protect Australia’s national security.*”

Within this definition, Northrop Grumman Australia recommends defence industry be categorised as a ‘regulated critical infrastructure entity’ due to its contribution to supporting ADF capabilities during times of national and regional crises.

Australia’s defence industry covers a broad scope of entities with varying capabilities and information security requirements. These requirements are dependent upon the classification of data, intellectual property and design work these entities hold or are engaged in. Noting the varying levels of security requirements inherent in Australia’s defence industry, Northrop Grumman Australia recommends that amendments to the *Security of Critical Infrastructure Act 2018* provide the Australian government with the scope to flexibly designate specific defence industry entities as a higher ‘entity level’ classification than the designation given to the wider sector. This flexible application of classifications recognises that there are entities within the sector that would be inadvertently burdened by a higher tier of critical infrastructure classification, where their work is at arms-length engagement with projects; for example, manufacturers producing a specific component that will be integrated into a more advanced platform. This varied classification concept could be applied on a temporary or permanent basis depending on the work being undertaken and should be considered on a case-by-case basis.

Recommendation 2: The Australian government should codify Australia’s defence industry as regulated critical infrastructure.

Recommendation 3: The Australian government should be enabled, through the *Security of Critical Infrastructure Act 2018,* to flexibly designate (permanently or temporarily) specific defence industry critical infrastructure entities as a higher ‘entity level’ classification than the wider sector.

CATEGORISATION OF OTHER CRITICAL INFRASTRUCTURE SECTORS

Northrop Grumman Australia considers the proposed list of identified critical infrastructure sectors will strengthen Australia's overall national resilience. However, it is unclear if this list of sectors adequately captures some of Australia's critical environmental sectors, for example, meteorology.

The Bureau of Meteorology and other associated entities provide the government with real-time weather intelligence to support domestic and international operations, including humanitarian and disaster relief activities. Most recently, these organisations provided critical intelligence and assessments of national climate risks and projections during the 2019-20 national bushfire crisis, to inform disaster management and reduction strategies in support of national state and territory decision-making processes. Meteorology services are considered a critical national resource, and are a target of malicious cyber actors seeking to disable critical information systems during national climate and environmental emergencies – with potentially devasting effects. In 2016, the Australian Cyber Security Centre reported[3] that a foreign actor installed malicious software on the Australian Bureau of Meteorology's computer system to steal sensitive documents and compromise other government networks. Northrop Grumman Australia has worked with the Bureau of Meteorology since their breach to uplift their cyber resilience and increase their technical cybersecurity efforts.

The increasing frequency and severity of national climate-related disasters – coupled with the growing risk of meteorology network disruptions and cyber attacks – means that the meteorology sector should be designated as a specific critical infrastructure sector with proportionate security obligations. Likewise, it is important that other sectors and organisations that perform critical, time-sensitive, public service functions are aptly captured in this reform process.

Recommendation 4: The Australian government should expand the list of critical infrastructure sectors under the proposed legislative reform process to include meteorology, and consider the addition of other relevant public service entities.

PUBLIC-PRIVATE COLLABORATION TO SUPPORT UPLIFT

Bolstering the cyber worthiness of Australia's critical infrastructure will be central to our future security and economic success. In order to grow these capabilities, Northrop Grumman Australia agrees with the government's approach to develop a cooperative framework between government and the private sector to support a resilience uplift.

Greater public-private partnerships will improve the government's ability to reform the regulatory environment, set standards to secure Australia's cyber preparedness and resilience, and ensure that expectations on both service providers and end users are clear and transparent.

The successful, ongoing cooperation between Northrop Grumman Australia and ANU (see Case Study) provides a useful model to assess the range of activities identified in the Consultation Paper to improve critical infrastructure and government engagement. These include co-designing best practice guidance, providing whole-of-government threat assessments and briefings to industry, vulnerability assessments, briefings to boards of critical infrastructure entities on vulnerabilities and obligations, secondment programs and improving ministerial visibility on collaboration through enhanced reporting mechanisms.

Northrop Grumman Australia supports the collaborative approach outlined in the Consultation Paper in order to harness the strengths of public and private organisations. Like the Northrop Grumman Australia and ANU partnership model, this approach should be focussed on assisting entities to develop their own internal cyber culture and skillsets to increase, maintain and monitor their cyber resilience.

Additionally, Northrop Grumman Australia recommends that the Australian Cyber Security Centre (ACSC) coordinate the establishment of 'tiger teams', to support the critical incident response against advanced

[3] 2016 ACSC Annual Cyber Threat Report, Australian Cyber Security Centre, retrieved from https://www.cyber.gov.au/sites/default/files/2019-04/ACSC_Threat_Report_2016.pdf

persistent threats and attacks on critical infrastructure entities. The ACSC would coordinate these teams and provide the government and industry with rapidly deployable resources to conduct the immediate incident response required to counter cyber intrusions.

Due to the complexity of cyber systems and capabilities, Australia is currently facing a significant skills shortage in the cyber security sector.[4] In spite of education providers increasing access to cyber security skilling courses, this growth is not sufficient to meet the shortfall. In addition to the workforce shortfall, a lack of cyber literacy across the Australian population goes to the heart of the problems inherent with building a cyber-aware nation. The ANU attack was a reminder that systems and ICT investment are not enough, with strong security awareness and practices required across an organisation to reduce the risk of cyber compromise.

It is commonly stated that humans are the weak link in the chain when it comes to cyber security. Consequently, there needs to be concerted action to develop a cyber-aware culture that places responsibility on every employee, not just the 'ICT Department'. Parallels can be drawn to the way in which the work health and safety culture has permeated Australia, initiating in construction, but now an important aspect of every workplace. To bridge the skills gaps in cyber and raise cyber literacy across the population, the Australian government should look for opportunities to partner with industry to deliver cyber education programs that range from schools-based activities to workforce training and public awareness campaigns for the broader Australian society. These programs should also grow Australians' general digital health awareness.

Developing a cyber-aware culture is critical to building national resilience in critical infrastructure sectors. The latest *ACSC Annual Cyber Threat Report 2019-20*[5] has identified that a malicious email is the most common type of cyber security incident, accounting for 27 per cent of all reported incidents. Acknowledging the importance of developing cyber literacy and attracting the next generation of Australia's cyber security workforce, Northrop Grumman Australia established our annual CyberTaipan[6] competition in 2018. This cyber security initiative tasks young Australians and high school teams with finding cyber security vulnerabilities whilst conducting system hardening and critical maintenance exercises. Reports from our complementary US program, CyberPatriot, have found that participants are far more likely to feed into the cyber security and technical workforce in their career pathways.

As the Australian population becomes more cyber aware, there are opportunities to further develop these schools-based programs through greater public-private partnerships, to encourage students to pursue education and careers in cyber security and other science, technology, engineering and mathematics (STEM) disciplines.

Recommendation 5: The Australian government should work with industry to design, develop and implement the collaborative critical infrastructure activities identified in the Consultation Paper to support cyber resilience uplift.

Recommendation 6: The Australian Cyber Security Centre should establish and coordinate 'on-call' joint public-private tiger teams to respond rapidly to advanced persistent threats and large-scale cyber attacks on critical infrastructure entities.

Recommendation 7: The Australian government should consider opportunities to support and partner with industry to develop and deliver cyber education initiatives to attract the next generation of cyber professionals.

[4] Australia's Cyber Security Sector Competitiveness Plan, AustCyber, retrieved from https://www.austcyber.com/resources/sector-competitiveness-plan/executive-summary.

[5] ACSC Annual Cyber Threat Report July 2019 to June 2020, Australian Cyber Security Centre, retrieved from https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf.

[6] Northrop Grumman Expands Youth Cyber Education Program into Australia with CyberTaipan, 25 June 2018, Northrop Grumman, retrieved from https://news.northropgrumman.com/news/releases/northrop-grumman-expands-youth-cyber-education-program-into-australia-with-cybertaipan.

INITIATIVE 1: POSITIVE SECURITY OBLIGATIONS

The first of three initiatives proposed by the government under the enhanced critical infrastructure regulatory framework – as outlined in the Consultation Paper – is establishing positive security obligations for critical infrastructure entities, supported by sector-specific requirements. The Positive Security Obligation (PSO) will propose a set of principles-based outcomes, including identifying and understanding risks, mitigating risks to prevent incidents, minimising the impacts of realised incidents and effective governance. Security obligations include physical, cyber, personnel and supply chain security.

Government represents a large element of Australia's critical infrastructure and must be an exemplar. The Protective Security Policy Framework (PSPF) and the related Information Security Manual (ISM) sets out the requirements for protective security to ensure the secure continuous delivery of government business. The PSPF and ISM also apply to industry providing goods and services for government departments and agencies. If the PSPF and ISM represent Government's best practice then it should be used to provide guidance for CI and SONS.

Northrop Grumman Australia recommends the development of a risk framework for cyber worthiness that would complement the PSPF and ISM, to inform the principles-based outcomes sought through the implementation of the PSO initiatives. This framework should identify commonalities across all critical infrastructure sectors and seek to develop a complementary maturity framework, which can assess the cyber preparedness of critical infrastructure entities and whole sectors, to guide the prioritisation and deliver of initiatives under the critical infrastructure reform process. An essential element of this approach would be system modelling, to determine the acceptable level of reduced operational capacity for entities within a critical infrastructure sector, which would provide a baseline for operations.

In the case of the ANU cyber attack (see Case Study), the Australian Strategic Policy Institute (ASPI) noted[7] that the attack was only detected when the university invested in upgrading the "normal" cybersecurity measures in place across its networks and carried out a "baseline threat hunting exercise". Through the PSOs, similar measures should be recommended to all critical infrastructure entities to help mitigate their vulnerability to cyber threats.

ASPI reinforced that a key lesson from the ANU case study was that organisations need to go beyond standard protective security such as firewalls, anti-virus measures and intrusion detection software, and consider whether they need more proactive measures within and across their internal systems.

Northrop Grumman Australia supports the Consultation Paper's PSO initiatives and welcomes the application of clear and concise security requirements. However, a broader cultural shift is also required that will be difficult to simply impose on regulated critical infrastructure entities and systems of national significance. This cultural change would see entities across the spectrum of regulated critical infrastructure adopt a similar approach to security as their counterparts in defence industry, where the requirement of a security clearance instils a responsible, cyber-aware approach.

Recommendation 8: That the PSPF and ISM represent Government's best practice then it should be used to provide guidance for CI and SONS.

Recommendation 9: The Australian government should work with cyber industry experts to develop a risk framework, and corresponding maturity framework, to assess the cyber preparedness of critical infrastructure sectors and ensure the consistent application of Positive Security Obligations across the various sectors.

Recommendation 10: The Australian government should develop and implement a comprehensive engagement strategy targeted at critical infrastructure sectors and entities to enhance cyber awareness and culture.

[7] Shoebridge, Michael "Lessons from the ANU cyberattack", The Strategist, 4 October 2019, retrieved from https://www.aspistrategist.org.au/lessons-from-the-anu-cyberattack/

Recommendation 11: Critical infrastructure entities subject to Positive Security Obligations should be required to examine their baseline level of security and conduct regular health checks to ensure an appropriate level of maturity is in place.

REGULATORS

The Consultation Paper proposes the appointment of sector-specific regulators to design and enforce regulatory standards for critical infrastructure sectors. These regulators would be responsible for co-designing security standards, educating industry about sector standards, and monitoring and enforcing standards (including through issuing penalties). Northrop Grumman Australia supports this approach, and recommends that regulators ensure consistencies across the different sectors in accordance with the level of regulation applied to them.

Current regulators may have a different focus on safety and may require an uplift in cyber skills to be able to ensure overarching regulation within sectors. It is important to note that safety critical system requirements can sometimes be at odds with cyber security and may require risk managed trade-offs to be considered. Northrop Grumman Australia supports the appointment of cyber regulators for each critical infrastructure sector, as outlined in the Consultation Paper. However, there are inherent complexities in the remit of regulators that presents an opportunity for the government to draw upon the expertise that can be provided by industry partners who have experience in large-scale enterprise cyber reform. For this reason, it is recommended that strategic industry partners are selected to assist regulators with implementing and monitoring the PSOs. It may be suitable to select an expert partner for each of the identified sectors that will be impacted by the proposed legislative reforms.

For any regulatory function to be effective, the standards need to be clear. Within the ICT and cyber industries standards vary significantly. Through Northrop Grumman Australia's work with the NSW Cyber Security Standards Group, we are consolidating the multitude of cyber standards to deliver a consistent, industry-focused cyber security framework for NSW. In the same vein, Northrop Grumman Australia recommends that sector regulators work cooperatively to adopt common standards for cyber security across Australia.

Once a common set of standards has been agreed, Northrop Grumman Australia recommends that regulators work with industry partners to assess critical infrastructure entities and their maturity against the standards. This assessment process should be revisited periodically to measure an entity's progress and performance in line with the standards.

While many critical infrastructure sectors already have regulators, these will not necessarily possess a familiarity with cyber security since this may be beyond their remit. As such, an uplift in the capability and capacity of regulators will be required in order to administer this duty. In addition to appointing or expanding the remit of sector regulators, consideration should be given to appointing an overarching "system architect" with responsibility for ensuring common security standards and metrics are appropriately applied across critical infrastructure sectors. Consideration also needs to be given to the question of what is being regulated: is it the maturity of an entity's system and security culture, or the entity's role within the entire critical infrastructure ecosystem? Northrop Grumman Australia's view is that it should be both.

Throughout the regulatory process, communication and consultation with industry will be a vital function of the regulators. It is important that regulators engage regularly with industry through workshops, briefings, newsletters and forums, to ensure critical infrastructure sectors and entities are supported through the legislative transition and remain abreast of any changes to their security obligations.

Recommendation 12: The Australian government should appoint critical infrastructure cyber security sector regulators, with a clearly defined role and remit. Regulators should be encouraged to establish strategic partnerships with industry, to support the development, delivery, assessment and ongoing regulation of the Positive Security Obligations for each sector.

Recommendation 13: The Australian government should implement a "systems architect" to oversee the regulation of the entire critical infrastructure system and enforce a common set of standards for critical infrastructure security.

INITIATIVE 2: ENHANCED CYBER SECURITY OBLIGATIONS

Under the proposed framework, the Australian government is considering the establishment of an information-sharing capability with entities classified as 'systems of national significance', in order to inform and develop a near real-time national threat picture. This would empower these entities to take appropriate and timely action against threats and help to establish an aggregated threat picture for the government to develop a more comprehensive understanding of the risks to critical infrastructure.

The Australian government has proposed that this framework operate on a voluntary basis in the initial phase, with a view to eventually mandating the provision of information about networks and systems if requested. The goal is to improve Australia's cyber threat situational awareness in order to strengthen the ability of critical infrastructure entities to reduce the risk and impact of a significant cyber attack.

Northrop Grumman Australia agrees with the mandatory reporting obligations proposed in the Consultation Paper for entities categorised as 'systems of national significance'. Additionally, the Australian government should encourage other critical infrastructure entities to publicly report cyber incidents, to help raise public awareness and alert critical sectors to possible threats. In the case of the ANU cyber attack, ASPI saw the subsequent public report[8] published by the ANU as the start of a "healthy shift" for institutions in publishing details of cyber incidents and their responses. It said greater openness about such incidents would build a body of knowledge and good practice, as well as building trust in the institutions holding personal data.

Northrop Grumman Australia has observed that the stigma and potential reputational damage to Australian companies of reporting a cyber breach is reducing. This attitude is likely to encourage greater uptake of a voluntary reporting mechanism. Northrop Grumman Australia also recognises that the messaging around sharing reports of a cyber breach is becoming more positive, and that the transparency will not adversely impact future government work. However, this will need to be maintained in order to continue to build a transparent, cyber-responsible industry to work in partnership with government.

Recommendation 14: The Australian government should mandate the reporting of cyber incidences to entities categorised as 'systems of national significance' and encourage voluntary information-sharing by all critical infrastructure entities to support the development of a national threat picture.

Recommendation 15: The Australian government should work with industry to de-stigmatise cyber incident reporting.

Recommendation 16: The Australian government should encourage all critical infrastructure entities to participate in a voluntary framework of enhanced cyber security obligations, beyond those designated as 'systems of national significance'.

SECTOR PLAYBOOKS

Under this second initiative, the government has proposed the co-design of industry preparatory activities such as industry playbooks, in order to assess industry's vulnerabilities and cyberworthiness, and guide industry and government responses to a range of cyber threat scenarios.

Critical infrastructure entities recognise that immediate action is required to protect vital assets in the event of a network intrusion. Clearly defined playbooks and scenario response planning would equip entities with the requisite knowledge to action the necessary first steps in protecting their networks in the event of an attack. These resources will assist critical infrastructure sectors to respond to threats proactively, within the limits of their cyber expertise, and commence defensive actions while government-industry 'tiger teams' are requested and assembled to support an entity.

Northrop Grumman Australia is well-positioned to assist the Department of Home Affairs and the ACSC in developing incident response playbooks that can be crafted to suit a broad cross-section of sectors. Our expertise is underpinned by our proven track record of assisting industry and government partners to respond to advanced persistent threats, and establish enduring processes and procedures to enhance

[8] Incident Report On The Breach Of The Australian National University's Administrative Systems, Office of the Chief Information Security Officer, ANU, retrieved from https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

security posture. Ultimately, critical infrastructure entities need to strive for a level of cyber maturity across their people, processes and technology.

Recommendation 17: The Australian government, Department of Home Affairs and Australian Cyber Security Centre should engage strategic industry partners with experience and expertise in managing the entire spectrum of cyber intrusions through to critical incident response, to ensure cyber playbooks are fit for purpose.

INITIATIVE 3: GOVERNMENT CYBER ASSISTANCE FOR ENTITIES

Under this initiative, the government has proposed a three-step response model to protect critical infrastructure from, and mitigate the effects of, cyber attacks. This spectrum of responses ranges from industry-initiated action, to government-mandated action through to government-controlled action. Under the highest-level response, the government would be able to declare a cyber emergency to deal with an immediate and serious cyber threat to Australia's economy, security or sovereignty.

Northrop Grumman Australia supports this approach, however, recommends that the Australian government consider broadening the critical incident response team to include cyber-mature private organisations. Organisations such as Northrop Grumman Australia and other high-end Australian cyber organisations have the ability to work with government to coordinate critical incident responses in their sectors of expertise.

Northrop Grumman Australia recommends that as the Australian government, the Department of Home Affairs and the Australian Cyber Security Centre develop critical response processes that are informed through strong partnership with industry experts. Developing these partnerships early will better enable the government to augment its cyber incident response teams with the support of trusted industry partners such as Northrop Grumman Australia, in defence of Australia's critical infrastructure.

Recommendation 18: The Australian government, Department of Home Affairs and Australian Cyber Security Centre should engage expert industry partners to assist in delivering strong, decisive cyber effects in the event of a cyber intrusion on an Australian critical infrastructure entity.

CONCLUSION

Northrop Grumman Australia commends the federal government on taking the initiative in moving to strengthen the cyberworthiness of Australia's critical infrastructure. These sectors represent a weak point that a malicious actor can use to undermine our ability to function as a society and protect our interests and their protection from attack is vital.

In our response, we emphasise the critical role that defence industry plays in enabling the ADF to carry out its duties, both internationally and – increasingly – domestically as it assists in disaster relief and pandemic responses. The incapacitation of Australia's defence industry through a cyber attack would have a profound impact on the ADF's capability and therefore warrants its inclusion as a critical infrastructure sector.

A central theme throughout our response has been the need for cultural changes, both in the value placed on cyber security by employees in critical infrastructure, and in industry's willingness to be open and transparent about cyber threats and attacks. As we have found through our own experiences with the Australian National University and the Bureau of Meteorology, greater transparency builds trust, and encourages others to consider their own security measures.

In all of these areas, Australia's private sector is well-placed to work with the government to provide the skills, the knowledge and the first-hand experience to meet the challenge of defending Australia's critical infrastructure from cyber attack.