LOCKHEED MARTIN
Australia

Australia's 2020 Cyber Security Strategy

Consultation and comment
29 October 2019

Prepared by:
Lockheed Martin Australia & New Zealand
8 Brisbane Avenue
Barton, ACT, 2600
[redacted]
www.lockheedmartin.com.au

Summary Statement

To summarise the opinion of Lockheed Martin Australia, there are four things to consider:

1. The threat landscape has changed, the situation is challenging, evolving and multifaceted;

2. The current policy and compliance settings actively undermine information sharing, which could be a major weapon in countering cyber-attacks/intrusions;

3. Balance between a compliance- and risk management-based approach; and

4. Policy standards that promote growth of cyber education through industry engagement and education reform.

Lockheed Martin Australia appreciates the opportunity to respond the Department of Home Affairs Cyber Security Strategy 2020 Paper (Cyber Strategy) and believes that there are significant opportunities to support the Australian Government and the community at large.

Overview

Lockheed Martin Australia is an Australian company that is engaged in research, design, development, integration and sustainment of advanced technology systems, products and services.

We are an industry leader in defence and technology, working with Australian and international partners to bring best practice and leading-edge concepts and technology to Australia.

As defence industry leader, Lockheed Martin Australia provides products and services that address some of the world's most critical issues. But our contribution doesn't end with a commitment to support Australia's national security and defence and economic growth.

Lockheed Martin Australia are delivering full-spectrum cyber capabilities and cyber resilient systems to our defence, intelligence community and global security customers. Lockheed Martin Australia is inspired by their missions and we're dedicated to helping governments and militaries around the world protect their platforms, systems, networks and data.

From initial concept to life-cycle sustainment, we consider and integrate full spectrum cyber capabilities into everything we deliver to our customers. Lockheed Martin Australia builds the platforms, tradecraft and tools that are proven to make them move faster, be safer, improve quality and contain costs for critical cyber missions.

Lockheed Martin delivers Cyber Services globally to military and commercial engagements including:

- Cross Domain Solutions;
- Cyber Electronic Warfare;
- Cyber Kill Chain;
- Cyber Resiliency; and
- Computer Incident Response Team (LM-CIRT).

As a responsible corporate citizen, we also play an active role in helping to strengthen the quality of life in our country and the communities where we live and work. We partner with Australia's leading universities and the Defence Science and Technology Group and have established a multidisciplinary research and development centre – STELaRLab – recognising Australia's reputation for world class research.

Our investment in local communities and STEM initiatives create opportunities for thousands of Australians to enjoy a better future. We're committed to a community relations program that invests in the quality of life of communities where our employees work and live. Advancing STEM is a critical focus as our future success depends on a constant supply of highly trained highly capable talent for the nation. We are dedicated to supporting and improving the lives of those, and the families of those that have served and sacrificed for our country.

In responding to the questions raised by the Cyber Strategy, Lockheed Martin Australia has identified three distinct areas on which we would like to comment:

A. Landscape and Engagement;
B. Supply Chain and Compliance; and
C. Training and Education.

Part A - Landscape and Engagement

What is your view of the cyber threat environment?

The cyber threat environment is constantly changing as more and more sensors and intelligence sources become available human intelligence (HUMINT) blends with signal intelligence (SIGINT); automation of intelligence sources and analysis is much more available; and open-source communities continue to improve the usefulness of commodity tools. The environment continues to evolve, and defensive tactics must advance continuously.

Australia's small companies involved in cyber security provide a critical role in our national cyber defences. However, while our small-to-mid sized suppliers have the advantage of agility, they do not have the resources to properly defend against Nation State adversaries. Industry at all levels and Government must collaborate to achieve a more comprehensive and persistent national cyber defence.

LMA believes such Australian Government initiatives as the Department of Industry Defence Industry Cyber Maturity questionnaire (C3FDI) collaborative effort, in which LMA is involved, should be fostered and funded further to uplift Australian defence suppliers' capabilities.

Due to the ever-growing interconnectedness, including in military platforms, the potential impact of a cyber incident to Australia and Australian interests is increasing. More than ever, the need to embed cyber resilience, and not just cyber security, in all aspects of business and industry in Australia is increasing.

What threats should Government be focusing on?

Threats emerge at both the tactical and strategic levels constantly and from a wide range of actors and sources. Government should focus on ways to collaborate better within itself and with industry to combat threats that pose significant risk and impact to critical infrastructure, including finance, energy and defence. Defenders must be able to leverage not only intelligence from within their own environments, but that of government and industry.

As threats like ransomware become much more accessible to malicious actors, not always driven by nation-states, additional priority needs to be placed on resiliency and recovery.

The need for constant vigilance and awareness of the next level of aggressors requires an agile and dynamic focus that allows for the unexpected or unique approach to be considered as a normal course of business rather than extraordinary.

The work undertaken by the Australian Cyber Security Centre (ACSC) and the Joint Cyber Security Centre (JCSC) model has helped to improve ICT security in many sectors. The defence engineering sector has benefited from improved means for sharing threat information, ensuring engineering and design of Australia's new defence acquisitions are more resilient to the threats they are likely to face in the future.

Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
Do you think the way these responsibilities are currently allocated is right?
What changes should we consider?
What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

How can Government maintain trust from the Australian community when using its cyber security capabilities?
What customer protections should apply to the security of cyber goods and services?

Regarding the balance of responsibility for managing the risks, Lockheed Martin Australia agrees that in a constantly shifting environment and with the need for dynamic reaction ever increasing, the responsibility for managing the threat within the modern landscape is going to require new thinking, effective coordination and strong leadership.

The Government is in the business of maintaining the civil order and legislative processes while maintaining liberties and freedom of choice within the larger community. Economic growth relies on the Government providing policy, standards and guidance that provides assurance to this growth mindset, while at the same time balancing the need to respect civil liberties.

In recent times there has been a continuous evolution of policy, as the Protective Security Policy Framework (PSPF) has shifted focus from whole-of-government to whole-of-economy. The emphasis is for the PSPF to be supported and taken up by, small and medium enterprises (SMEs) and the broader industry, which has not proven to be effective as there is no obvious or demonstrable return on investment for commercial entities, despite Government advice around the increasing threat landscape.

This focus on compliance with the Australian Government's Policy Framework is complicated for multinational organisation, who are required to comply with international standards and regulations from a plethora of countries and regulatory bodies.

Adoption of global standards, such as the ISO27001 framework, NIST's Special Publication (SP) 800 series or CNSS Security model, will allow more scope for the Government to allocate resources to the more critical requirements of classified environment and critical infrastructure. This approach will allow refocus of resources on the immediacy of responding based on credible intel that is available through interagency agreements and sharing of sources that are beyond the scope of the commercial and industrial community in isolation.

Additionally, the policy has evolved to the point where there are a number of government bodies with responsibilities for cyber (in some way shape or form). In the case of defence industry this has resulted in a fragmented and inconsistent approach that is often contradictory, incomplete, and not cohesive.

While the Australian Government Information Security Manual (ISM)'s move to a risk-based approach is welcome; it's monthly update cycle is not workable and completely impractical for defence industry enterprises. The eventual replacement of the ISM, which is anticipated to be NIST for defence, should be brought forward to remove ambiguity.

What role can Government and industry play in supporting the cyber security of consumers?
How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?
Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

Consumers seek assurance from the government that an industry is providing integrity in its services. Recent history suggests that the global public is losing confidence in Government institutions and regulators.

The cyber security industry has seen considerable growth and expansion, as technologies become faster and powerful infrastructure becomes more ubiquitous. Government cannot offer all of the solutions on its own and in many cases, agencies that seek to do so incur significant cost, time delay and limitations on what they can provide. Successful partnerships need to be developed between government agencies and industry to bring solutions forward in a timely and responsive manner. Care must be taken however in developing these partnerships, because with little oversight there is a plethora of companies claiming to offer the "silver bullet" solution while not being able to prove the reality behind the solution.

The current initiative of the ACSC to implement the MSP Partner Program (MSP3) serves as a positive offering and paves the way to establish a "white list" or assurance position that consumers of security services that reference to ensure security across the broader industry. This program has the potential to build partnerships between Government and industry that allows for solutions to be rapidly developed and – more importantly – evolved as the threats evolve in a cost-effective and timely manner.

Increased awareness campaigns, additional resources to public facing agencies that support and protect business and consumers at all levels will boost the levels of integrity and assurance in a rapidly expanding industry.

Government could consider removing from the ACSC\ASD model, small business and economic cyber security concerns, which would allow a greater focus on critical infrastructure and national security.

Small business and economy would perhaps be better managed through government-industry partnerships:

- Grants to support cyber hygiene improvements (ie funded pen-testing or vulnerability assessments);

- Awareness activities driven by industry with light touch government support;

- MSPs and ISPs having greater accountability forced onto them for protecting consumers;

- Mentoring programs with Government recognised and endorsed companies.

The JCSC model also needs to become more dynamic and responsive to needs of the broader community. It is acknowledged that its very existence is a step in the right direction and has helped improve awareness – it just needs to be less of a drop-in centre and more tailored to improving capability.

Part B - Supply Chain and Compliance

Is the regulatory environment for cyber security appropriate? Why or why not?
What specific market incentives or regulatory changes should Government consider?
What needs to be done so that cyber security is 'built in' to digital goods and services?

The traditional posture of the Australian Government through the PSPF and the Information Security Manual (ISM) has been enforcement through checklist compliance methodology. The objective of the PSPF and ISM are to achieve a balance between a risk-based approach and a compliance-based mitigation. Recent changes to the PSPF and ISM have seen a shift from a compliance methodology, which has led to a reduction in visibility of the risk realisation. This has led to Government departments and agencies to rely on policy writers to focus their IT spending decisions. This distracted from the true source of risk and threat to the agency.

In recent years, with the shift towards risk-based decisions and away from strict compliance, government departments and agencies are becoming more averse to sharing and collaboration at the risk of compromise of loss of information, while the demand for information sharing and transparency continues to increase.

The overall move to a risk-based approach appears to have tried to address the wider approach of those organisations that needed to align to the ISM (ie state governments, and organisations managing government data such as cloud providers) but not highly-classified systems.

If the Government can better balance the mix of compliance and risk awareness, there would be greater levels of opportunity for collaboration and information sharing, which leads to greater capacity to counter cyber adversaries.

Lockheed Martin as a primary supplier to the United States Department of Defense (DoD) and the United States of America (US) Government continues to demonstrate compliance with the ISO27001 and NIST 800 SP1 standards as part of our ongoing commitment to maintaining the highest level of assurance.

All current contractual engagements require us to maintain this compliance and demonstrate commitment to these standards through internal and external audit undertakings. The US Government engaged DoD throughout these reviews to ensure our undertakings meet their expectations and foster continuous growth and transparency.

Lockheed Martin's approach to this problem has been to design and embed contemporary processes to design in resilience to cyber threats into its systems engineering approach. This approach recognises that cyber incidents will occur, and thus the focus is more on the capability to detect, react and recover than the typical cyber security approach of identity and protect.

Lockheed Martin has previously undertaken a series of training sessions with Australian industry to highlight the supply chain risks from a cyber security standpoint. This training was undertaken with the Centre for Defence Industry Capability (CDIC) and quickly identified an immaturity in terms of a) how industry could move towards protecting itself and b) what the threat environment looked like. Lockheed Martin Australia then worked with the Commonwealth to focus on strategically important supply chain partners for further analysis with the eventual uptake of the initiative led by the now CDIC.

How could we approach instilling better trust in ICT supply chains?

The US Government identified the need for increased ICT supply chain confidence, which resulted in the release of the Federal Acquisition Regulation (FAR). The FAR contains the principal set of rules, which governs the process executive agencies of the U.S. Government acquire goods and services by contract with appropriated funds. A supplement to the FAR called the Defense Federal Acquisition Regulation Supplement (DFARS) provides DoD-specific acquisition regulations that contractors doing business with DoD must follow in the procurement process for goods and services.

In 2015, the U.S. DoD issued a contract supplement for defence contractors and subcontractors regarding the protection of unclassified Covered Defense Information (CDI) and the reporting of cyber incidents occurring on unclassified information systems that contain CDI. The specific supplement is the Cyber DFARS 252.204-7012 which has been in force since December 2017.

This clause replaced the Unclassified Controlled Technical Information Rule, imposing new baseline security standards and significantly expanding the information that is subject to safeguarding and can trigger reporting requirements. The most commonly referenced additions are the inclusion of 110 controls documented in NIST 800-171 (Special Publication Revision 1).

Lockheed Martin created the internal Corporate Information Security (CIS) Cyber DFARS Program Office to coordinate and drive the various communications, IT programs, business area specific needs, government engagement and supply chain initiatives associated with the new cyber regulations. The updated requirements impose new baseline security standards and significantly expands the information that is subject to safeguarding and reporting requirements. Most controls noted in the Cyber DFARS are already in place for enterprise and business area wide systems, and the CIS Cyber DFARS Program Office is working with Lockheed Martin's global supply chain organization and business areas to evaluate and facilitate compliance with the regulations by our suppliers and for our program specific IT environments (e.g. labs). In addition, CIS has taken an industry-leading role in working with the DoD and Lockheed Martin's trusted defence industrial base partners to collaborate on the interpretation and implementation of Cyber DFARS.

Government could be more open with Defence Industry about their whitelists and blacklists. The ACSC Cyber Supply Chain Risk Management Guide was a good start but is too broad. An industry specific approach (for critical infrastructure and defence industry) would be welcome, particularly the instances where Government may direct an organisation not to use a certain supplier or broader provider of service (e.g. no components with supply chains from certain country of origin etc).

Lockheed Martin Australia would also acknowledge the joint industry and government (Dept Industry) approach to determining defence industry supplier maturity (C3FDI) Program. It would be good to see next steps of this program take the outputs from primes and resource targeted initiatives to lift the security resilience of Australian suppliers so that they are more mature in protecting themselves and Australia's interests and more competitive overall.

Part C Training and Education

How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

It is document[1]ed that there is a significant gap in the knowledge and skills set currently in the security industry, both in government and private sectors.

The future cyber security professionals are being educated and trained through the high schools and university courses of today, for tomorrow. The exponential growth of malicious actors can only be curtailed through the introduction of unique thinking and opportunity into the next generation of professionals and leaders.

Lockheed Martin Australia acknowledges this gap in skills and knowledge and is actively engaged through outreach activities into schools through the government-based STEM initiatives, STELaRLab university challenges and engagement of top tier graduates and academics.

There is a need to grow cyber talent, in Australia and beyond, and Lockheed has identified a number of models and potential growth opportunities including:

- CyberFirst is part of the National Cyber Security Centre with a purpose to grow young cyber talent in the UK https://www.cyberfirst.ncsc.gov.uk/ ;
- Lockheed Martin Australia is actively engaged in the LM global CyberQuest and CodeQuest - competitions that aim to inspire high school students to pursue careers in cybersecurity and coding;
- Universities need to ensure ICT and Engineering disciplines are contemporary and have cyber electives. The current offering of cyber-specific undergraduate and post-graduate courses are usually too broad and not relevant to the skills required currently and with little future proofing.

The Australian Government could consider allocating additional resources towards the educational initiatives such as these events (or similar), while maintaining the connection to industry and educational bodies.

While there a number of hurdles to the development of talent, the most commonly identified constraint is related to obtaining and maintaining security clearances. The process of obtaining clearance is often long and laborious, it is confusing for those that have never held a clearance and the single managed clearance process has never been fully realised due to capacity and funding constraints for the central body and other Government department's layering of additional requirements on the clearance process.

Streamlining and increasing the transparency of the clearance process will decrease the fear and trepidation behind holding a clearance, while maintaining the vigilance and rigour in the process. Maintaining clearance for high level environments is critical to ensuring the trust in classified system, however information sharing can be achieved through greater clarity in the

[1] https://www.industry.gov.au/data-and-publications/meeting-demand-for-cyber-security-expertise
https://www.abc.net.au/radio/programs/am/cyber-security-leaders-seek-solutions-for-dire-skills-shortage/11531322

classification process as over classification of information is the greatest constraint to successful sharing of information.

What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Collaboration and sharing of knowledge between industry and government cyber professionals is essential to ensure currency in the ability to identify future threats and vulnerabilities, and keep ahead of the malicious actors and operators.

The Australian Cyber Security Centre and Lockheed Martin Australia's Cyber Incident Response Team maintain a sound relationship and actively seek opportunities to engage with the ACSC and other prime providers of security services the Australian Government to maintain the proactive and immediate capabilities to respond to attacks.

One way of overcoming these constraints is to follow up on the previous initiative of PM&C during the early days of the exiting Cyber Strategy was to run several war games that involved cross sections of Government, industry, media and academia. These exercises improved awareness and introduced the concept of a combined response effort to a significant cyber incident.

It should also be acknowledged that State Governments have a role to play and it would be useful to see a cohesive approach. By way of an example, South Australia recently launched a Cyber Collaboration Centre with an objective of developing cyber security skills among others and sharing information amongst government, industry and specialist providers.

Government should continue these exercises and Lockheed Martin confirms its willingness to take part as a partner and trusted global citizen.

[redacted]

Joe North
Chief Executive
Lockheed Martin Australia & New Zealand
November 2019