MCAFEE ENTERPRISE

27 August 2021

Department of Home Affairs
techpolicy@homeaffairs.gov.au
Submitted online via: https://www.homeaffairs.gov.au

McAfee Enterprise's submission in relation to the 'Strengthening Australia's Cyber Security Regulations and Incentives' discussion paper.

McAfee Enterprise welcomes the opportunity to provide input to the Department of Home Affairs Call for Views paper - "Strengthening Australia's Cyber Security Regulations and Incentives," published by the Department of Home Affairs on July 13, 2021.

McAfee Enterprise, a world leading independent cybersecurity company, is focused on accelerating ubiquitous protection against security risks for businesses, and governments worldwide. Inspired by the power of working together, McAfee Enterprise creates cybersecurity solutions that make the world a safer place. McAfee Enterprise cloud security extends from device to cloud with data visibility, data loss prevention and advanced threat protection on a platform that supports an open ecosystem. Our holistic, automated, open security platform allows disparate products to co-exist, communicate, and share threat intelligence with each other across the digital landscape. We enable the convergence of machine automation with human intelligence so our customers can streamline workflows more efficiently, be freed from operational burdens and be empowered to strategically combat threats from adversaries.

Our response includes answers to specific questions asked, as well as general comments.

INTRODUCTION

In an environment in which global cyber threats, whether criminal or state-based in origin (or indeed an alliance between them) are fast-moving, coordinated, and high tech, we need to develop meaningful, sustainable, and responsive policies, strategies and systems that empower, rather than impede, national governments, corporations, cyber security vendors, small-to-medium enterprises, and indeed, the community as a whole, to defend against cyber-attacks.

The connections between and within national governments via interconnected digital infrastructure using standardized communication protocols have never been greater with the wholesale transition to cloud for many government agencies. In parallel, the links between individual devices (whether enterprise or BYOD) and these government and corporate systems

continues to grow exponentially: Gartner statistics predict there will be 25 billion IoT devices by the end of 2021, with some 60% of these in consumer hands.[1].

Our ongoing responses to these increasingly ubiquitous, global attacks on government and private data need to build equally strong global alliances and address a series of local needs.

Our existing intelligence sharing arrangements via the Five Eyes Alliance, provide an underlying architecture that connects like-minded nations in the struggle to combat these common threats. In July 2021, the Five Eyes nations made a joint statement on strategies to combat the threats cyber hackers posed to governments and citizens' data.[2] We know from experience that global alliances of this kind are critical elements in the battle to keep our data from the prying eyes of foreign security services and criminals.

In managing these threats, many governments around the world have also sought to harden policies around access to sensitive data, including the hardening of devices, hardening of access permissions around whose device may connect with which systems, data localization rules, and revised data sovereignty and data residency settings.

There can be serious unintended consequences to poorly implemented or poorly targeted policies. While these policies carry with them the powerful promise of more secure systems, it is critical that in the development of these defensive postures we remain cognizant of the compromises they represent in terms of our ability to respond to cyber threats, or other crises. These include:

- A reduction in available information will increase the risks from cyberattacks
- A cost increase for implementing and maintaining state-of-the-art tools across different localization regions
- Less choice in distributed storage solutions, which assist in deploying privacy, integrity, and counter-intrusion protocols on networks
- Some also argue that data localization interferes with fraud prevention. For example, the inability to mirror data across several data centres can prevent the provider from seeing patterns and trends of fraud or other risks.

As we develop a shared understanding of which policies and processes promote real cyber-security, we need to ensure we do not compromise our ability to scale platforms and services for global customers, continue to build interoperability between government departments, and lay the foundations for continued global operational effectiveness between national governments as

[1] Gartner, 'Gartner Identifies Top 10 Strategic IoT Technologies and Trends', 7 November 2018. Accessed online at: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

[2] Matthew Cranston, 'US and allies expose details of China's cyber attacks', *The Australian Financial Review*, 19 July 2021. Accessed online at https://www.afr.com/world/north-america/us-and-allies-to-expose-details-of-china-s-cyber-attacks-20210719-p58av3

we combat cybercrime and cyber-attacks. This in turn requires us to build on the systems, policies and products that work, and develop new ones that empower us to fight the threats these attacks pose.

As you will see in our responses below, we believe that actions need to be taken but that the efforts, this Call for Views addresses, should look to leverage the successful efforts which have occurred in allied countries. Wherever possible, look to incorporate the successes that have occurred elsewhere with the tailoring needed to adapt to the Australian needs. This will allow for faster and more successful outcomes. Below, we outline the reasonable steps the Australian Government can take to protect its systems, while simultaneously empowering private sector and community efforts to build a truly resilient cyber security eco-system.

GENERAL COMMENTS

As mentioned in the Quick Summary document, the Australian Government is "proposing three areas of action — *setting clear cyber security expectations; increasing transparency and disclosure; and protecting consumer rights*. To set clear minimum expectations we are considering greater use of cyber security standards for corporate governance, personal information, and smart devices. To increase transparency, we are considering initiatives on cyber security labelling for smart devices, vulnerability disclosure and health checks for small businesses. In the area of consumer rights, we are seeking your views about appropriate legal remedies for victims."

- McAfee Enterprise is pleased the government is committed to working together with industry to design new workable strategies and policies focused on strengthening cybersecurity within Australia.
- Industry and consumers are generally averse to additional regulation for regulation's sake. However, thoughtful regulations targeted at specific outcomes can be useful, as long as those regulations are reviewed and re-evaluated periodically to ensure they are delivering the desired results and they have not become outdated and counterproductive.
- The Call for Views identifies ransomware as a significant issue and highlights the importance of addressing it on a global basis. Dealing with the effects and results of ransomware will do little to stem the problem. Australia must work with its international partners in a concerted effort to address the underlying causes and to reduce the impact of ransomware on our digital ecosystem. An international effort, led by the Institute for Security & Technology, established the Ransomware Task Force (RTF)[3], comprising 60+ experts from industry, government, law enforcement, civil society, and international organisations. The RTF developed a comprehensive framework recommending policies and actions to 1) deter ransomware attacks, 2) disrupt the ransomware business model, 3) help organisations prepare and 4) respond to ransomware attacks more effectively. The report and recommendations are

[3] Ransomware Task Force - https://securityandtechnology.org/ransomwaretaskforce/

documented in the *Comprehensive Framework for Action*[4] and should be considered for use in conjunction with the efforts specified in this Call for Views paper. Ransomware is an international problem, not just an Australian problem and as such, requires a more globally coordinated effort. The US government has begun implementing the RTF recommendations as they pursue a whole of nation approach to the ransomware problem.

- In Section 2 of the 'Call for Views' it states, "technology companies may prioritise their own reputation and commercial interests over the interests of their customers". This is contrary to the principles and vision of McAfee Enterprise. We put customers at the core of everything we do. Our company tagline – Together is Power – is further evidence of the importance we place on designing solutions that improve the lives and businesses of those we protect. The view that cybersecurity companies, such as McAfee Enterprise, are not aware of the responsibility and trust placed in us, or that we would pass responsibility onto our customers is inaccurate.

  That said, there are things that the end users of any software should be aware of. Security is complex. As a cybersecurity vendor, we try to reduce the impact by assuring we hide complexity wherever possible. Configurations that are locally managed often provide a pathway for the attacker. Is it the vendor's problem when malicious actors find that the password set by the end user is "1234password", the name of their wife, or a common dictionary word? Phishing attacks of all sorts provide malicious actors access to the user's systems, simply because the user decides to click on the link that looks most interesting or appears at the top of their search result. Certain items are the local user's responsibility, with education being the key to minimising the impact. We are in a transition time between generations – those that have never had much experience with cyber devices, and those who cannot remember a time without them. It is essential that cybersecurity education starts as children enter the education system and continues throughout K-12 education. If that was the case, many security problems would disappear.

RESPONSES

1. Governance Standards for Large Businesses

– **What is the best approach to strengthening corporate governance of cyber security risk? Why?**

The best approach is to look around the globe and implement the solutions that have been most effective. It is simply easier and faster to leverage existing successes instead of going through the time-consuming process of creating something from scratch.

– **What cyber security support, if any, should be provided to directors of small and**

[4] RTF Report - https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

medium companies?

It should be understood that today's small companies are tomorrows rapidly growing enterprises. Small to medium sized companies should not be treated differently to large corporate entities. The processes needed to strengthen corporate governance are the same regardless of size. Introducing the need for cyber risk management as an integral part of overall businesses risk management processes, along with the protections it helps foster, will increase as the business grows.

The following section addresses both questions asked above.

Compliance versus Risk Management

It needs to be understood up front, that compliance is not security. Compliance programs as a direct means to an end are actually distracting from the overall goal of securing Australia. Compliance initiatives divert resources from actual security risk management. They tend to give senior executives a false sense that they are doing the right thing. "Are we compliant?" is the wrong question for corporate directors to be asking. "Are we doing what is needed to reduce cyber risks and threats to our company and our customers as effectively as possible?" is the mindset needed. Compliance enables corporate management to simply meet the minimum requirement, rather than do what is needed to address the threats and risks to the organisation. The focus needs to change from a compliance mindset to one of overall cyber risk management.

Cybersecurity Framework: an alignment & risk management foundation

While it is understood that businesses are vital to improving the cybersecurity landscape for Australia, it is important to understand that this is a shared problem. Businesses are particularly good at various aspects of "Corporate Risk Management," such as financial risks, environmental risks to corporate facilities, competitive risks, physical risks, dependency risks, risks to shareholders, etc. What needs to occur is the understanding that Cyber Risk Management should be and must be incorporated into any corporate risk management governance process.

This is not a new problem. This problem has existed in other parts of the globe. In the U.S., the NIST Cybersecurity Framework (CSF)[5] has become ubiquitous in its use. This U.S. initiated voluntary effort is being adopted globally and delivers the necessary impact by changing the dialog from "Compliance" to "Risk Management."

The CSF was developed as a voluntary cyber risk management governance standard for large U.S. critical infrastructure organisations. However, it was quickly apparent it was applicable in many types and sizes of organisations, both public and private. It was designed and developed by thousands of people from diverse parts of industry, academia and government participating. It is principles-based, not prescriptive and is

[5] NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

highly aligned with international standards. Sound familiar? These are exactly the same goals stated in the Call for Views paper as "One Possible Approach."

The focus of the CSF is to drive cybersecurity risk management discussions throughout all levels of an organisation and, in the U.S. and elsewhere, it has been highly successful. Corporate Boards from many diverse aspects of the economy are now incorporating more Board members with cybersecurity experience and backgrounds. Boards are discussing cyber risks, protections, and costs, while doing so with a level of comfort that these types of conversations did not allow in the past. Utilising the Cybersecurity Framework has allowed cyber risk management to be integrated into existing corporate risk management programs, and to do so without excessive costs.

— **Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?**

It is important for government and business to work together in a voluntary way that benefits both. Compliance is NOT security. It is a business checking a box to assure it is able to avoid penalties and continue operating. The problem is that compliance activities often take money away from the security budgets, and as such becomes counterproductive to achieving the longer-term goals of improving security. Governments have focused on compliance regimes and have given corporate leadership the impression that is the most important consideration. It is not. When the focus from governments changes to a cyber risk management perspective, businesses pay attention. Focusing on education and potential targeted legislation that makes Cyber Risk Management, using a tool such as the CSF, a Board level responsibility will be more effective. Assessing an organisation's complete cyber risk is not as expensive as it may sound. Once an organisation has a baseline, they can then see the impacts, both positive and negative, as to how they can address the cyber business risk to their organisation. Cyber Risk Management is just another category of Corporate Risk Management that the corporate board, and leadership must incorporate into their overall corporate governance.

Other Considerations

If the decision made is to not leverage previously successful efforts and instead, to create something from scratch, then there are some items we believe are needed to make the effort successful. The proposal for voluntary principles of cybersecurity governance for large businesses, co-designed with industry, is broadly in line with McAfee Enterprise and industry objectives. But:

- The cybersecurity industry should have a real role in the co-design / development process.

- Principles must align with existing cyber requirements in Australia and relevant international standards and best practices.
- Must be focused on levelling-up – improving understanding, skills, programs – rather than adding a layer of burdensome administration
- Should not be made mandatory, at least initially, while the utility of this approach is assessed.

Recommendation:

We recommend the Australian Government take advantage of the work that has preceded this Call for Views, such as the Cybersecurity Framework. At worst case, tailor the successful cyber risk management outcomes to better match the needs of Australia.

2. Minimum Standards for Personal Information

All organisations involved in providing services to and for consumers need to ensure they uphold the strictest standards when protecting the personal information they hold from misuse, interference, loss, and from unauthorized access, modification, or disclosure. We know that citizens are becoming more privacy aware and are placing more value on their digital footprint. Simultaneously, the ongoing threat of cyber-attacks means governments and businesses must remain vigilant on the need to protect personal information.

McAfee Enterprise has actively implemented enhanced privacy standards, controls, and processes throughout the company and incorporated them into our products and services to protect the personal information we are entrusted with. We are bound by and compliant with international privacy standards and frameworks. We provide transparency to our customers, consumers, and employees so they understand how we collect, use, handle and manage their personal data. We assist a range of organisations globally, including government departments and corporations, in their efforts to protect the personal information they hold.

The Australian Government Agencies Code, the Australian Privacy Principles, the Notifiable Data Breaches Scheme, and the Privacy Act (which enables them) already require companies to implement appropriate technical and organisational measures to protect personal data and outline courses for remedy in the event of a breach.

These are in line with global standards for the protection of personal information. We remain committed to upholding these strict standards in all jurisdictions in which we operate.

— **What technical controls should be included?**

Sadly, this is not a situation where a specific set of technical controls will totally address the problem. There must be a multi-pronged approach to properly address the protection of privacy of the personal information of our citizens. In addressing privacy and personal data protections, multiple approaches should be leveraged in parallel.

1. **Encouraging Privacy by Design**. Like security, it is critical that privacy controls are built in from the beginning of newly implemented processes and products. 'Privacy and Security by Design' requires companies to proactively consider privacy and security on the drawing board and throughout the development process for products and services introduced to the market. It also means protecting data through technology design that considers privacy engineering principles. This proactive approach is the most effective and efficient way to enable data protection because the data protection strategies are integrated into the technology as the product or service is created. McAfee Enterprise believes Privacy and Security by Design encourages accountability in the development of technologies, making certain that privacy and security are foundational components of the product and service development processes. But it is not just products and services where Privacy by Design principles should be leveraged. Internally when new operational processes are developed that touch consumer, customer, or employee data, it is critical that privacy principles and controls are incorporated.

2. **Encouraging using a privacy framework.** The use of an established privacy framework for development of internal privacy processes, or in establishing a privacy office, is needed to provide the organisation the ability to comply with the multiple international regulations. Examples include best practices developed, documented and available from the International Association of Privacy Professionals (IAPP)[6] and the U.S. NIST Privacy Framework[7] to name two. Privacy regulations are affecting organisations globally and assuring the organisation can comply with the diversity of regulations is critical. Utilising a privacy framework allows the organisation to meet the requirements of the global needs of their customers.

3. **Establish aligned privacy regulations and controls.** It is hoped the regulations and potential required controls instituted are aligned with other established effective international standards and regulations. Many Australian and multi-national companies serving Australia are already required to assure they comply with multiple international privacy laws, such as the General Data Protection

[6] IAPP - https://iapp.org/
[7] NIST Privacy Framework v1.0 https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework

Regulation (GDPR) (applicable to the European Economic Area) and the Personal Information Protection and Electronic Documents Act (Canada) to ensure individuals' right to privacy is protected in addition to the Privacy Act.

By leveraging all three approaches simultaneously, privacy protections can be effectively implemented and make a real difference.

– **Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken? Why or why not?**

Incorporating a cyber security code would have limitations that may impact future cyber security legislation. The cyber security focus would only be allowed to apply to personal information protections. It would be better to do the reverse. Privacy cannot be effectively implemented without real cyber security controls. In the U.S. NIST's Cyber Security Framework (CSF) was developed first. The NIST Privacy Framework leveraged the CSF to effectively describe the proper way to implement privacy protections. Maybe that is what is needed here, developing a cyber regulatory framework where the cyber security needs and controls are not limited to simply protecting personal information. This would provide the basis for future cyber security regulatory needs as the security landscape continues to evolve.

3. Standards for Smart Devices

– **What is the best approach to strengthening the cyber security of smart devices in Australia? Why?**

The Call for Views seems to limit the description of smart devices to just those targeted towards consumers. The reality is that smart devices span more than just consumer IoT, as many of the same components are incorporated into smart building automation, and thus beyond just the realm of consumers. Actions taken should target the broader market impact of these devices.

Voluntary approaches to these devices have not worked. Vendors often cite economic reasons for failure. They use the argument that the cost of the devices is so small that for the consumer, it is hard to justify security controls costs. For some suppliers, this is a bogus argument. While the specific consumer device may be cheap to make, there is a reason for that. They are doing the absolute minimum to get the product to market and while that may have been useful in the past, today there are too many knockoffs doing the same thing. Certain products are stand alone, while others have a backend infrastructure needed to provide the smart device enabled service. Something must be done to assure smart devices of all types, costs and complexity are properly secured. It seems the government would like

to establish security as a purchasing differentiator. To do so will require the mandatory approach to smart device standards. There is no reason to allow insecure smart device products to continue to be sold in Australia if the impact on the nations' digital landscape is to make the nation more insecure. Utilising appropriate international standards for supporting smart device security makes sense for Australia and the international community.

– **Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?**

ESTI EN 303 645 would most certainly be an appropriate international standard for Australia to adopt. The cybersecurity provisions within the standard are common sense based and needed so as not to allow an existing attack vector to continue. We cannot allow home users or building owners that utilize cheaper smart device automation to become the "soft insecure underbelly of Australia" that is constantly being attacked.

We do not believe that Australia should limit the implementation of ESTI EN 303 645 to simply three top requirements. Smart device vendors should be required to comply with all the cybersecurity provisions of the standard. The standard provides a framework for secure implementation and management of smart devices. You cannot simply pick and choose the top three and be successful. It is better to specify the need to comply with this standard to be able to sell into the Australian market.

– ***[For online marketplaces]* Would you be willing to voluntarily remove smart products fromyour marketplace that do not comply with a security standard?**

The authors of this response are not an online marketplace. However, it may be beneficial for products that comply with the Australian regulations for smart devices to have some visual means to convey this. This could be a label or a logo. It is critically important that consumers can distinguish between those products that do and those that do not comply.

– **What would the costs of a mandatory standard for smart devices be for consumers,manufacturers, retailers, wholesalers, and online marketplaces? Are they different from the international data presented in this paper?**

We believe this is the wrong question to be asking. What would be the costs to consumers and the nation if these types of common-sense cybersecurity provisions were not adopted? Cheap products may represent initial savings but end up costing considerably more to secure. Further, remediation costs may also be higher for substandard or low-cost smart devices. The increased protection of consumers' privacy, reduced identity theft and more secure smart home/smart building implementations would far outweigh the minor increase in product costs.

– **Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in**

this paper?

Not sure these are unintended consequences, but consequences such as:

- Increased costs to the consumer
- Costs to the government to assure online marketplaces understand their responsibilities under the new Australian smart device regulations
- Vendors having to invest to upgrade their products to comply
- Unfriendly nation vendors creating insecure or intentionally insecure smart devices as they see a market movement away from their sales

4. Labelling for Smart Devices

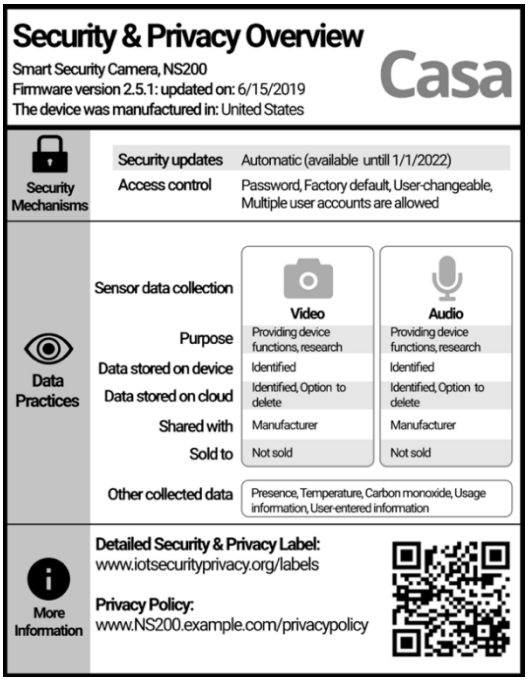
– **Is a label for smart devices the best approach to encouraging consumers to purchase secure smart devices? Why? If so, should it be voluntary or mandatory?**

A label on smart devices is a way to educate consumers to think in a manner that begins to make cyber security more of a mindset and a buying differentiator. While there are various studies on the effectiveness of labelling, the established labelling schemes are not operating in such a dynamic environment with vulnerabilities potentially discovered throughout the life of product.

Product labelling alone will likely not succeed as a policy initiative. The government would need to educate the citizens as to what the label is for, what it means and how to interpret the contents of the label. The Call for Views differentiates between voluntary labels and mandatory labels. It is hoped that the expiry information would also be incorporated into the cyber star label as well. While the mandatory, "support until" approach of the solely expiry date label is easier, it is also not going to produce the desired outcome in our opinion. If you are going to focus on trying to educate the buying public to use the labels to make an informed decision, then the labels must contain sufficient information to inform the user of the various aspects of cyber security and privacy.

For example: the following label is based on the work being done at Carnegie Mellon University Security and Privacy Institute[8]. It shows a label that is highly informative and useful when making a buying decision and includes expiry information as well.

[8] https://cylab.cmu.edu/news/2020/05/27-iot-labels-consumers.html



It also provides reference links, so the consumer can investigate further as to the security and privacy characteristics and capabilities of the smart device in question. The mandatory versus voluntary aspect is really an open question of effect and results. Voluntary will take hold, but it could take years for smart device product vendors to take note and consider implementing the label. Mandatory with a reasonable timeline for implementation will have a more immediate effect on the marketplace.

– **Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?**

Designed properly, the two will benefit each other. Labelling provides a transparent way for the product vendor to convey important security and privacy related information to the buying public. Standards provide the cyber security minimum baseline for cyber security characteristics and requirements for the product vendor to follow. Consumers already think products are secure out of the box. Requiring recognized international standards, will ensure products begin to live up to that assumption.

It should be noted that there are limitations to a labelling approach:

- Labels should target the capabilities of the product, as demonstrated in the sample label above.

- Labels SHOULD NOT BE stating that “this product is free of security vulnerabilities.” That gives the consumer a false sense of security that is not real. This approach will lead to the consumers losing trust and interest in the label if it is not viewed as current and factual.

- Products are evaluated and generated at a specific point in time and while they may be free of known vulnerabilities today, tomorrow a new vulnerability may be found in one of the components of the product. No product will be forever free of vulnerabilities.

- A process-focused approach is more effective. However, consumers must understand that doing the right things will not lead to perfect outcomes. A labelling scheme must manage this to avoid erosion of trust among consumers.

– **Should the label be digital and physical?**

The real question from our perspective is, why does this need to be an either-or question. The label should be both as needed. In some cases, the label could stand on its own, but most often, it will not be possible to depict the privacy and security aspects of the product to the consumer. Having reference URL link capabilities for those products that are in a box or physical package and sold in physical stores, provides the vendor with the ability to provide all the information they feel is needed.

– **Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?**

Any mandatory labelling regime should not cover traditional IT products, such as laptops, PCs, and other general purpose computing devices. Smart phones fit the latter category. Smart phones act as a platform for various types of software to run on. The individual applications that need to be installed on the general-purpose computing device need to have labels. These labels would be digital as these products are most often purchased via online marketplaces and app stores.

– **Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?**

As previously indicated, having both types of labels available to the manufacturer benefits both the company and the consumer. The manufacturer will not be forced to deal with deciding how to incorporate all the necessary security and privacy content into the footprint of the label. They can instead, provide all the needed information to the consumer via a QR code or a reference URL printed on the label. The Consumer benefits by having access to a much deeper set of information about the products handling of the consumer's personal information and the product's security characteristics. Having the option to use both types of labels, in concert or individually, assures the information is available to the consumer.

5. Responsible disclosure policies

Responsible disclosure policies, often referred to as Coordinated Vulnerability Disclosure (CVD), using documented Vulnerability Disclosure Processes (VDP), foster a controlled and transparent means for addressing vulnerabilities from discovery to remediation.

The proliferation of interdependent technologies in both hardware and software is creating a landscape where coordinated vulnerability disclosure and handling is more important than ever. CVD is currently recognised as a key cybersecurity activity, and existing standards and guidance have served the global community well in building a consensus around best practices. CVD provides an opportunity for vulnerable organisations to work with finders and reporters of vulnerabilities to analyse, mitigate, and communicate security flaws publicly, leading to a more positive resolution than if the vulnerabilities were not addressed or if organisations and vulnerability reporters do not collaborate. That said, additional work needs to be done to ensure the connected world can effectively manage an increasing number of critical vulnerabilities that must be communicated to another party for remediation or mitigation.

While we agree and are actively encouraging responsible disclosure processes in many different arenas and have a founding member of the Common Vulnerability and Exposures (CVE) Board from McAfee Enterprise, it is important to understand the scope of the problem accurately. The research used as the basis for the statement, "*However, US research indicates that 50 percent of vulnerabilities remained without a patch for more than 438 days and that vendors did not always prioritise the highest risk vulnerabilities*" is highly misleading and inaccurate as the research[9] only looked at open-source projects and their code repositories. It did not look at actual commercial products. Commercial product vendors are not volunteers when it comes to developing software. The products are commercially sold and as such have incentives to be responsive to their customers. Commercial software vendors have Product Security Incident Response Teams (PSIRTs) and structured supported processes in place to assure they can effective and quickly deal with discovered vulnerabilities in their products.

Additionally, responsible disclosure policies should not be focused entirely on software or hardware vendors. Often vulnerabilities are discovered in a business's online presence. In those cases, business need to have the means in place to assure the vulnerability reporter has a structured, discoverable, and supported means to notify the organisation of the vulnerability with the expectation it will be corrected and without fear of retribution of any kind.

– **Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?**

The Call for Views discussion paper has documented the components that need to be implemented in parallel. McAfee Enterprise believes the government should take a blended approach to encouraging coordinated vulnerability disclosure processes within the business community.

---

[9] Frank Li and Vern Paxson, "A Large-Scale Empirical Study of Security Patches" (University of California, Berkeley, and International Computer Science Institute, 2017), https://www.icir.org/vern/papers/patch-study.ccs17.pdf

1. Communicate clearly and widely that the government desires businesses to develop and integrate a structured and public CVD / Vulnerability Disclosure process for receiving appropriate vulnerability information from external reporters.
2. Leverage existing regulations to reinforce the incorporation and use of CVD/VDP processes.
3. The Government should create a template / toolkit for businesses to use as the basis for their CVD program and distribute it directly to every business. Pushing it into the business's organisation will have more impact, while at the same time giving the business a place from which to start. It is much easier for a business to tailor something than to create it from scratch, especially when they are not sure what it is they are creating. The toolkit should include educational materials that cover both the public and internal side of a CVD program. It is important to provide the business an understanding what a CVD program consists of, what they need to do internally to make the VDP process effective, and what is needed to be considered when tailoring the toolkit's supplied public vulnerability disclosure process documentation. Businesses will need to understand the process so that they can properly assign and establish the process internally.
4. The government should set up a website focused on responsible disclosure / Coordinated Vulnerability Disclosure. It should have links to the toolkit and additional references to both Australian and international vulnerability disclosure educational resources. The site could also provide a quick registration for businesses that have established and posted a public vulnerability disclosure policy. This could be used by vulnerability reporters to know where to go to report a discovered vulnerability in a product or business infrastructure. This publication could also act as an incentive for some to register and be seen as doing the right thing for their customer. This type of registration should be initially voluntary.

At the same time, this must not be just about the business landscape. The government needs to assure they too are complying and leading by example. There is precedent for this. The U.S. government mandated every US federal agency and the DoD have published and public VDP policies. The Office of Management and Budget published an "Improving Vulnerability Identification, Management, and Remediation10" memorandum to all agency heads stating "*VDPs establish processes for the identification, management, and remediation of security vulnerabilities uncovered by security researchers. They are among the most effective methods for obtaining new insights regarding security vulnerability information and provide high return on investment. They also provide protection for those who uncover these vulnerabilities by differentiating between good-faith security research and unacceptable means of gathering security information. VDPs establish processes and procedures for the security research community to report vulnerabilities to appropriate agency contacts, who can then use the reports to address vulnerabilities of which they may not have been aware.*"

[10] OMB Memo M-20-32 - https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

The Australian government should publicly do something similar in assuring vulnerability finders can coordinate discovered vulnerabilities in a structured way by following an established and published public process.

Considerable progress has already been made in international standard setting bodies around vulnerability discovery, disclosure, and remediation, and as such the government should ensure they leverage existing standards such as ISO/IEC 29147:201811 and ISO/IEC 30111:201912.

6. Health checks for small businesses

Every business is dependent on far-reaching supply chains, and we have already seen some serious cyber incidents resulting from security lapses. Historically, supply chain professionals focused on protecting links through supplier qualification, insurance, physical security, and protecting against risks ranging from theft to delayed deliveries. While those practices remain essential, today's supply chain professional must add a focus on information security to their defensive strategy. These efforts need to focus on protecting intellectual property, defending against hacktivism and espionage, detecting embedded malware, and ensuring continuity of operations.

One of the best ways of ensuring the "cyber-security" health of small businesses is for government and corporate "buyers" to establish clear rules for participants in their supply chain. Not all small businesses are equal, and it is important to understand and identify needs and vulnerabilities. The corner fish shop, for example, will have different needs and represent different vulnerabilities compared to a specialist consultancy supplying services to the Australian Department of Defence.

The processes for managing security risks in the supply chain are akin to the processes for ensuring quality. The first step is to identify and classify each link in the supply chain with regards to what they do now and the critical aspects of their contractual obligations. Then clear baselines of security and privacy requirements need to be established for the group. Standards tools such as ISO/IEC 27036 (information security for supplier relationships) can provide a solid baseline.

Government departments and large corporations increasingly manage these risks through supply chain management processes. The Australia Department of Defence has requirements in place under the Defence Industry Security Program (DISP), managed by the Defence Industry Security Office (DISO), which supports Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts, and tenders.

With baselines established, the next step is regular validation of security and privacy controls. Validation can be challenging, full of competing acronyms, contractual issues, and

[11] ISO/IEC 29147:2018 - https://www.iso.org/standard/72311.html
[12] ISO/IEC 30111:2019 - https://www.iso.org/standard/69725.html

resource constraints. Doing this for every supplier in the supply chain is unrealistic for most companies, so it is important to prioritise. Fortunately, there are standards and processes emerging for various industries that range from self-assessment to third-party certification.

One example is the Cloud Security Alliance's Security, Trust, and Assurance Registry (STAR) for various cloud computing offerings. STAR is a straightforward three-level certification, accompanied by a publicly accessible registry. STAR provides valuable information about product certifications, including the date, country, term, and level of certification. Decisions can be based on a simple cost and risk comparison, or on more thorough analysis of the strengths and weaknesses of current or potential suppliers. Analogous to ratings systems in other industries such as banking or tourism, STAR requires little technical training to understand the difference between level 1, 2, and 3 certifications.

A range of similar programs are offered across Australia. Network providers such as Telstra offer health checks as a service for their clients across industry. The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) offers grants for small businesses to access cyber security testing, under the Cyber Security Small Business Program.

– **Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?**

The Call for Views states, "*During consultation on the Cyber Security Strategy, small businesses told us that they face a consistent set of challenges – limited time, limited money and limited cyber security expertise. This means that small businesses don't have as much opportunity to understand and implement existing guidance from the Australian Cyber Security Centre. As a result, small businesses are less likely to implement basic, but important, cyber security measures. This also means that many large businesses often don't have appropriate knowledge about the cyber security of important small business suppliers and customers.*"

Looking at successful international efforts to address this problem is an approach we recommend. We believe a program fashioned after the U.K.'s Cyber Essentials program could help small business better position themselves to operate more securely and understand their cyber responsibilities to their customers and their business.

– **Would small businesses benefit commercially from a voluntary health check? Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?**

We believe that a program such as described in the Call for Views would benefit all, not just the smaller business commercially. Larger businesses need to be made to understand the supplier risks to their businesses. By encouraging larger businesses to implement requirements into their supplier agreements requiring the suppliers to successfully

participate in a Cyber Health Check program the smaller suppliers are incentivized to participate. Working with those organisations that provide insurance to small businesses could also provide a means to get a wider adoption. Supplier security is critical and those purchasing from smaller suppliers should have some means of determining that a supplier is aware of their specific cyber risk responsibilities.

– **What other incentives would be required to encourage uptake? Is there anything else we should consider in the design of a health check program?**

It must not be a set and forget program. Small businesses should be required to renew their successful participation yearly in order to continue to keep up with the requirements of cyber security and the program. Some oversight needs to be in place to actively encourage participation, its value to the economy and to assure small business are not abusing the program.

– **Is there anything else we should consider in the design of a health check program?**

We recommend engaging and leveraging the experience of the U.K. government's Cyber Essentials program to learn from both their positive and negative aspects with implementing and running the program.

7. Clear Legal Remedies for Consumers

The issue of clear legal remedies for consumers in the event of a breach remains a vexed question for cyber security planners. Around the world, the policy settings governing data protection and privacy are evolving rapidly. The frameworks in Europe (GDPR) and Australia (NDBR, APP et al), create overarching legal frameworks for redress in instances of negligence, failure to notify, and others. The United States is more convoluted with an overlay of Federal Trade Commission (FTC), consumer (including health insurance) and other protections, and state and federal law – although the National Institute of Science and Technology (NIST) has developed a privacy framework in recent years. Across the common law jurisdictions, there is an emerging case law on these matters and existing remedies for consumers, although the cost of litigation can be prohibitive.

McAfee Enterprise believes that appropriate privacy protections are a key enabler of productivity and the appropriate use of technology.

For many organisations around the world, the introduction of mandatory reporting requirements for eligible data breaches highlighted where their privacy compliance gaps were, and triggered wholesale internal reviews of company data protection practices. There remains a way to go, but all organisations should uphold the strictest standards when protecting personal information and face consequences where they have breached the laws and regulations governing this critical area.

The ultimate arbiter of whether they have put in place appropriate protections for citizens and consumers is trust, and recent global history shows us that where that trust is broken, an organisation will likely face fierce outcry. This is true for both governments and corporations. We believe that trust in the integrity of systems – whether a corporate firewall or a child's cell phone – is essential to allowing individuals and corporations to benefit most from the power of technology.

While the protection of personal information and the need for redress remain front of mind for McAfee Enterprise (e.g., "Privacy by Design principles"), our key consideration is where breaches of personal information become vectors for broader attacks on the government and corporations. Our data protection and security solutions enable our corporate and government customers to more efficiently and effectively comply with applicable regulatory regimes.

– **Are the reforms already being considered to the ACL and Privacy Act to protect consumers online sufficient for cyber security? Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?**

McAfee Enterprise supports the desire to provide greater clarity to consumers concerning recourse in bringing actions and class actions against companies following a cyber security incident, where there is evidence the company responsible knowingly did not have an appropriate level of cybersecurity protections in place. The problem with this is that as cyber security evolves, companies are at times in an arms race to keep up with the malicious actors. There is a real difference in companies that are breached and have been trying to keep up, versus those companies that are totally failing to consider cyber risks to their business and their customers.

Those companies that have been the subject of a breach are themselves a victim and will suffer reputational damage and the response costs of clean-up and remediation. There should be real clarity as to when consumers could seek remedies through the Privacy Act and ACL. Without clarity on the conditions when consumers can seek legal remedies, companies will also now be faced with increased legal costs and judicial distractions to the business.

CONCLUSION

McAfee Enterprise thanks the Cyber, Digital and Technology Policy Division for allowing us to contribute our thoughts and recommendations to the dialog. As the conversation around these topics continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that you have the input and

background needed to successfully drive consistent, effective cyber risk management practices for Australia's future.

Please feel free to contact Cameron Ord, Federal Account Director (Canberra) at [redacted], and Craig Nielsen, Vice President, Asia Pacific at [redacted] at any time.

Respectfully submitted,

McAfee Enterprise