Submission to Home Affairs' Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives

Introducing Forum of Australasian Security Executives (FASE)

This response is a collective view from FASE to address the issues raised and make recommendations in response to the discussion paper.

Founded under the name SECMAN in 1999 and expanded and renamed in 2016, FASE has evolved into a professional affiliation of corporate security executives, occupying the most senior national and/or regional security role in their organisation; with responsibilities relating primarily to Security and Business Continuity Management, inclusive of Crisis and Emergency Management. Members other functional responsibilities may include internal investigations, fraud, cyber security and operational risk management. There are 50+ member companies (company names provided on request), with national and/or international standing with of individual annual turnovers in excess of one billion dollars.
FASE aims to achieve three primary goals in its pursuit of security best practice; by sharing knowledge and insights in the following ways:

- Promoting a trusted environment for Australian corporate security executives to discuss contemporary and strategic security threats and risks;
- Ensure collaborative engagement with all levels of Government and industry stakeholders on strategic security issues; and
- Provide security leadership and trusted advice on matters of national strategic importance by harnessing the collective experience, knowledge and resources of its members.

FASE achieves its primary goals by:

- Giving due consideration to emerging strategic risks from a security and resilience perspective;
- Ensuring the role of CSO or similar, now well established in corporate Australia, is constantly reviewed and assessed to ensure it remains contemporary and relative to the current and emerging security landscape;
- Taking a truly global perspective, in recognition that many members have global roles within Australian domiciled entities, by interfacing with like global Security organisations such as ISMA;
- Maintain FASE, in the minds of regulators and security agencies, as the 'go to' forum for Corporate Security in Australia; and
- Continuing to adjust and broaden its scope to encompass additional areas managed by its members including resilience, privacy, cyber, enterprise risk, assurance, governance/compliance, reputation and brand performance.

Our response

FASE is fully supportive of government and private sector initiative to improve national and industry cyber security practice supported by guidance and effective regulation but with minimal regulatory impact. A positive impact is less likely to be achieved by a regulatory "big stick" but rather through clarity of cyber security objectives, incentives and support for industry. Suggestions for incentives and support are in the body of this response. Given the role of FASE a number of the questions addressed are limited in comment as they were considered out of scope with our goals as an institution.

Question 1: What are the factors preventing the adoption of cyber security best practice in Australia?

FASE suggests that there are multiple significant factors preventing the adoption of cyber security best practice. Four which and are addressed below.

Diversity of guidance

There are a range of standards, national and international, propriety, governmental established and institutional from professional bodies. The consequence is that cyber security best practice has no "point of truth". You cannot follow best practice if you cannot find authoritative guidance. The material to develop a national guidance is available by providing an integrating framework for these various approaches. We suggest that cyber security principles, with guidance on implementation, can be achieved by reference to existing standards and revising and simplifying guidance in the Information Security Manual. A merging of key elements from the ISO/IEC 27000 series, the ISM and the NIST cyber security risk management framework and its supporting standards into an integrating principles and core process guide would be a significant step forward.

Training and awareness will not bring about enhanced security until the above issues are addressed. Secondly, the failure to address security holistically means that even with good digital protection and response, the cyber systems and their contents are still vulnerable, unless information security assessment and value allocation, physical security and personnel security are effectively converged with Cyber through the lens of a human factors focus. Members of FASE are happy to discuss this approach and its application.

Diversity Rate of change of application software, firmware and hardware

As inferred above the rate of change in applications, firmware requirements and hardware creates uncertainty in the user community as to the security way forward. Much of this change is profit derived profit driven change rather than capability driven. There are multiple capabilities on a security practitioner's desktop that are really for specialist use but their presence creates vulnerabilities and those that are regularly used create vulnerabilities when upgraded.

Digital technology is changing at such a rate that to keep up would be like trying to trade your car more often than once year because the capability and the safety systems are no longer sufficient or have been superseded by software vendors removing support for the product. Forced obsolescence for profit is a major cost driver.

Particularly the requirement to continually upgrade cyber defences, at a cost, as variation of older exploits mutate and there is no patching for legacy systems. For small and medium enterprises, the upgrade of networked legacy system can be prohibitive. The move to annually "leased" software will also create additional costs compared to previous purchase and licensing arrangements

Cost Level and availability of competent expertise

As suggest above cost is a factor reducing the uptake of best practice. This is true for individual business applications and even more so for enterprise systems. Best practice requires high level

gateway and systems defence, forensic capability, threat and risk analysis and response. In addition to the software, risk advice, maintenance of redundancy and recovery and "sand boxing" techniques the cost of skilled practitioners is becoming prohibitively expensive, even f you can find them.

The cost of maintaining an adequate protective security system for cyber in in the order of AUD$6 million. Current actionable threat advice from a reputable supplier in in eh order of AUD$200,000 per annum.

Security Magazine reported in 2021:

> ***Security Operations Centres (SOCs) Can't Meet the Rate of Security Analyst Turnover****: Despite organizations surveyed expecting to hire an average of five analysts in 2021, three will resign or be fired in one year. Organizations are increasing security analyst salaries, with the average rising from $102,000 in 2019 to $111,000 in 2020. However, only 38% still believe they can hire the right talent due to increasing complexity and rising security engineering and management outsourcing costs.*
>
> - ***Perceived ROI of the SOC is Dropping Due to Management Complexity****: More than half (51%) of respondents say the ROI of the SOC is getting worse, compared to 44% in 2019. More than 80% rate their SOC's complexity as very high, rising from 74% in 2019.*
> - ***Rising Outsourcing Costs Lessen Appeal:*** *The cost to pay MSSPs for security monitoring also increased and may impact ROI. The average cost for respondents is $5,307,250 annually, an increase from $4,441,500 in 2019 (i.e., approximately 20% year over year).*
> - ***High Security Engineering Costs Aren't Resolving Needs****: Organizations surveyed are spending an average of $2,716,514 per year on security engineering. However, only 51% of respondents rate their security engineering efforts as effective or very effective.*
>
> https://www.securitymagazine.com/articles/94413-the-economics-of-the-security-operations-center-whats-the-true-cost

The government will need to find a satisfactory solution for a Security Operations Centre model that is an active voluntary engagement with priority cyber business users and supports such enterprises according to risk based needs.

Complex threat environment

Little needs to be said about threat actors and their capability and intent, whether a nation state or criminal or a blend of them both. The NIST Information Technology Laboratory in its ITL Bulletin of May 2017 outlines an effective Cyber Threat Intelligence and Information Sharing model that could be adapted should the provision of timely threat intelligence and its delivery be facilitated by government.

A **security management program** is a security governance function designed to address **security-related risks** that threaten **business operations** and in turn **business objectives**

A **security management program** is incorporated into **business operations**, and assists **business continuity**

A **security management program** incorporates principles of **protective security** and the convergence of physical, personnel, cyber and information security

Security convergence involves the interaction and integration of security domains across all levels of the organisation, in accordance with the key objectives and accountabilities outlined in the **security management program**

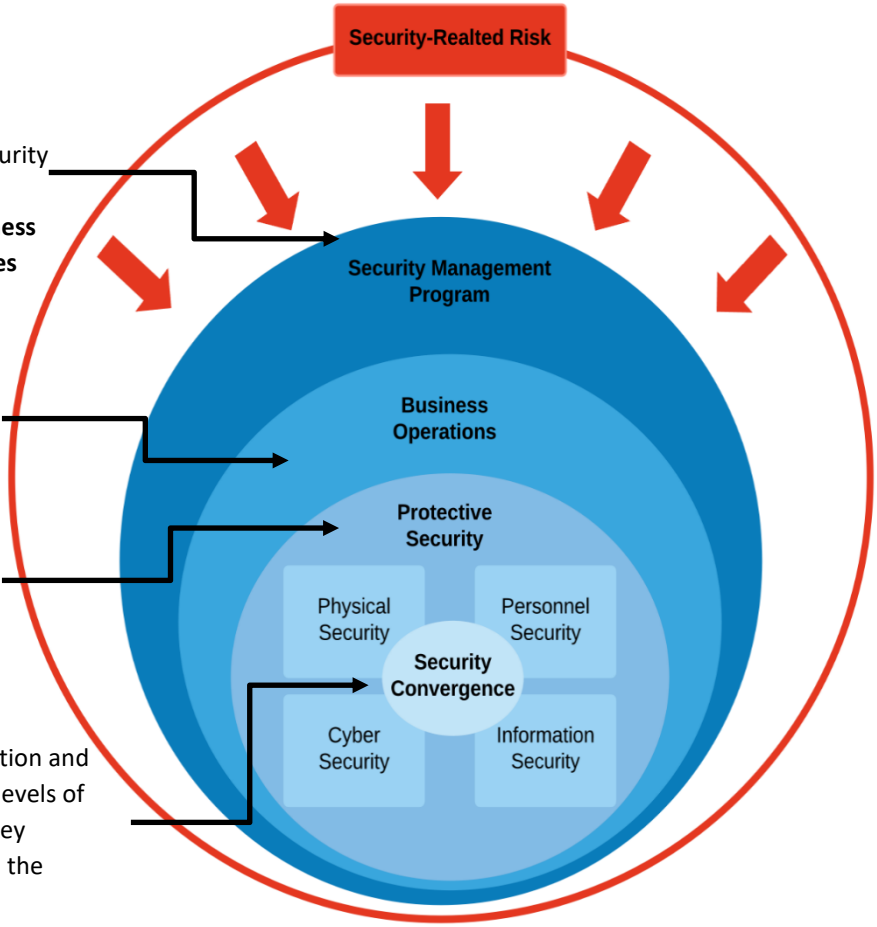

Diagram 1.0 - Security, Business and Risk Relationship Convergence Model

Bronte Munro 2021

Recommendation: *Following a detailed analysis of underlying problems and root causes for cyber security incidents and Government should properly assess the relevant principles that can be identified in a security system and implement a program to reduce the impact of inhibitors and encourage investment is support of best practices.*

Consideration should be given to enhancing government support for capability and response and a reward and recognition system (carrot not stick) for those striving to enhance their security, (e.g. tax incentives for cyber security enhancement).

Question 2: Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

If we take the view that a negative externality occurs when a cost spills over. A positive externality occurs when a benefit spills over. So, externalities occur when some of the costs or benefits of a transaction fall on someone other than the producer or the consumer. A cyber security failure will not just create a disbenefit for the business that suffers the failure, it will clearly impact along the supply chain and the stakeholders it services. In analysing the level of security required, the risks associated with this element need to be considered. An obvious approach is to address this in guidance for tendering and contractual requirements with specific

cyber security performance.

Asymmetric information arises when one party to an economic transaction has more or better information than another and uses that to their advantage. This is particularly true in high technology areas such a cyber service and infrastructure. It seems that much is taken on faith with many businesses doing insufficient analysis to understand the risk

There are other solutions other than the introduction of regulations. Alternative solutions include, offering warranties or guarantees on items sold or services provided, cyber insurance, and bottom-up efforts to inform consumers of products' and sellers' quality and reputation. The later of these goes to the training and awareness issues mentioned above and the creation of a sufficient volume of shared knowledge. Rather than regulations, government support for his type of approach may also be more cost effective and less resisted by business.

Recommendation: *Non-regulatory solutions to address inhibitors and support businesses to in cyber security and responding to cyber security incidents should have priority. The government provision of advice and guidance based on current and sustained knowledge base that is freely available to business.*

Question 3 and 4: What are the strengths and limitations of Australia's current regulatory framework for cyber security? How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

A major weakness is the diffusion of responsibility and accountability based on legislative silos. A cyber security breach will have multiple consequences and may therefore require reporting under propose SOCI, ASIC APRA and Privacy. Such diffused reporting prevents an effective integration of consequences of the event and is housed in stove pipes limiting the capacity of analysis of the broad effects.

Enhancing efficiency and effectiveness would indicate that government should have a single point for cyber incident reporting that would collect the relevant data for existing regulatory reporting and distribute accordingly while having the analytical capacity to analysis all implications of the breach. This element could be readily aligned to the regulatory, provision of guidance, benchmarking and reporting of status and compliance. This approach to the cyber reporting which represents the needs of regulators, would reduce the complexity for both for industry and government.

The FASE comments from our SOCI submission included below reflect this direction.

> *Regulators may not have expertise in the relevant areas of security, emergency management, crisis management and supply chain. A regulator may be acceptable to take the notification for self-certification or attestation, but the above issue of security expertise applies and, where there is more than one regulator, this creates a problem of multiple reporting and advice. A single reporting for point of entry should be available for multi sector industries and/or where the regulator does not have the requirements already in their regulations.*
>
> *The experience with SOCI was that the "rules" (regulations) didn't come until later in the process and the response received to any queries to the Regulator was generally not report on it all, i.e. They were not clear on what compliance looked like so just asked for everything.*

This incurred a additional internal work unnecessarily and external expenditure with risk and compliance consultants and legal advice to understand the legislation.

Similarly, Aviation & Maritime Security Team within DHA is already set up and managing MTOFSA, and Critical Infrastructure Centre managing SoCI compliance. Either one of these or collaboration between both under DHA could work. At present however both teams are overly focussed on compliance, and very little engagement is experienced by operators in support or proactive engagement and assistance

Regulators, if they be required to report on security requirements, should only be extended to provide a reporting mechanism for confirmation of alignment to PSOs or attestation/certification.

The consultation paper recognises that the Government's role is not just compliance and that a strong business culture, embracing security and resilience, with an appropriate framework for national critical infrastructure can only be built on relationships and co-operation between business and government agencies, i.e. sharing Intelligence assessments and lessons learnt, supporting with responses, guidance on best practice, fostering cross industry collaboration and co-operation, target hardening advice. We suggest that government agencies (regulators) get pre-occupied with the risk of compromising their ability to hold organisations to account for non-compliance with regulatory

Recommendation: *The Government should give serious consideration to setting up a single point of contact, backed by experts in cyber security and management and teamed with other security specialists. The Department of Home Affairs would be a possible location for a Protective Security Centre for advice and reporting. In addition, it could support training, standardisation and business and community awareness. It should have no law enforcement function but should be supported by ASIO ASD/ACSC and have access to data derived from police sources that can provide analytical insights. (FASE would welcome further discussion on the concept which would also be applicable to the SOCI reporting requirements).*

Question 5: What is the best approach to strengthening corporate governance of cyber security risk? Why? Question 6: What cyber security support, if any, should be provided to directors of small and medium companies? Question 7: Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Corporate Governance should be approached from an integrated security perspective but the issues around cyber related risk need particular emphasis. This is because we have lived with physical security and personal security issues for centuries. Cyber has a complexity and range of known, emerging and unknown vulnerabilities, rapidly changing as it is capabilities emerge in its functionality, within mega "systems of systems" (the Net, Telecommunications, satellite systems, etc) it has considerable issues around uncertainty and hence is difficult to understand and manage.

Governance arrangements are critical for security generally and given the above, an understanding of cyber relate risks requires special consideration from the Board down.

To ensure that a business can achieve its security objectives, accountability and responsibility must be allocated. In a small organisation it may be the Owner or Chief Executive Officer who is both accountable and responsible. In a larger or more complex organisation consideration should be made to appointing a security executive position, often referred to as the Chief Security Officer (CSO). The person appointed Security Executive, from here on CSO used, is delegated their responsibility by the

Chief Executive Officer or similar senior manager. The Role of the CSO should be highly visible and central to delivering on strategic business priorities and objectives.

CSO ongoing Responsibilities include;

- Ensure the protection of the business's personnel, material and intellectual assets in all forms, comply with national and international security regulations.
- Security procedures and practices are robust and of proven effectiveness
- Assist in the attribution of value to business assets in order to ensure security threats
- Ensure appropriate physical security measures are in place at all sites
- Ensure that all appropriate personnel security requirements are in place at all sites.
- Ensure that appropriate cybersecurity measures are in place at all sites
- Comprehensive approach to managing security incidents including investigating to determine root causes and inform security improvements and education programs.
- ensures personnel resources are deployed to support the maintenance of effective protective security; appointing skilled personnel according to business needs.
- Lead the network of security managers and directs resources and priorities across the business.
- Conduct security assurance activities of the business.
- Ensure security awareness training and education for the personnel of these entities are undertaken. All personnel are trained annually on security policy and procedures and take responsibility for implementation within their area of responsibility.
- Security culture is underpinned by continuous improvement and accountability

The relevant security principles and processes should be supported and advised by government and outreach and education programs at each level of an enterprise from awareness to security competence. Government should support the development of a protective security curricula in partnership with business and academia.

Recommendation; *The government should develop programs to assist Boards and owners to understand how they may effectively meet their governance responsibilities for the security of the business and establish a plan or mechanism to implement policy and procedures throughout their business.*

Question 8: 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? Question 9: What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)? Question 10: What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

The Privacy Act is too limited in its focus and scope to be the best, or even a suitable, vehicle for enhancing cyber security in business. Privacy reporting is important but a more holistic approach is required. The preferred outcome is that businesses achieve and maintain a security outcome for themselves and stakeholders (Including in many cases the broader australian society). Staying in business and being successful, without negative consequences, is a prime objective. Achievement of this objective by a business will mean the privacy concerns are addressed. The nation would be better served by government supporting businesses to achieve secure outcomes rather than mandating specific results.

Recommendation: A general code indicating outcome expectations, security principles and core

process expectations is preferred to sector specific regulatory changes that may have unexpected consequences and limited positive impact.

Question 11: What is the best approach to strengthening the cyber security of smart devices in Australia? Why? Question 12: Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?

- ***a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?***
- ***b. If not, what standard should be considered?***

Several forecasts indicate that IoT will connect 50 billion devices worldwide by the year 2020. There are a number of possible application areas, such as smart city, smart grid, smart home/building, digital agriculture, smart manufacturing, intelligent transport system, e-Health. IoT is an enabling technology that consists of many supporting technologies, for example, different types of communication networking technologies, information technologies, sensing and control technologies, software technologies, device/hardware technologies. This referenced document is based on widely used enabling technologies that are defined in standards from several organizations such as ISO, IEC, ITU, IETF, IEEE, ETSI, 3GPP, W3C, etc.

Trustworthiness is recognized as an area of importance, and IoT can leverage current and future best practice. For example, monitoring and analysing deployed IoT systems is essential to maintain reliability and safety and security. Measures such as controlled access can ensure the security of the system.

ISO/IEC provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high-level system based reference with subsequent dissection of that model into the four architecture views (functional view, system view, networking view and usage view) from different perspectives.

This document serves as a base from which to develop (specify) context specific IoT architectures and thence actual systems. The contexts can be of different kinds but shall include the business context, the regulatory context and the technological context, e.g. industry verticals, technological requirements and/or nation-specific requirement sets.

The **ETSI EN 303 645**, created by the European Standards Organization 'ETSI', is **a standard specifically designed for consumer Internet-of-Things (IoT) devices**. The standard while useful but should be compared and aligned to ISO/IEC 21823-1:2019(E) provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a common understanding of interoperability as it applies to IoT systems and the various entities within them.

Further the architecture of IoT devices and connectivity is addressed in ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture. Also ISO/IEC 21823-1:2019 provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a

common understanding of interoperability as it applies to IoT systems and the various entities within them.

NIST is also providing comprehensive guidance in this area:

- **Draft NIST SP 800-213**, ***IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements***, has background and recommendations to help federal agencies consider how an IoT device they plan to acquire can integrate into a federal information system. IoT devices and their support for security controls are presented in the context of organizational and system risk management. SP 800-213 provides guidance on considering system security from the device perspective. This allows for the identification of IoT device cybersecurity requirements—the abilities and actions a federal agency will expect from an IoT device and its manufacturer and/or third parties, respectively.

- **Draft NISTIR 8259B**, ***IoT Non-Technical Supporting Capability Core Baseline***, complements the NISTIR 8259A device cybersecurity core baseline by detailing additional, non-technical supporting activities typically needed from manufacturers and/or associated third parties. This non-technical baseline collects and makes explicit supporting capabilities like documentation, training, customer feedback, etc.

- **Draft NISTIR 8259C**, ***Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline***, describes a process, usable by any organization, that starts with the core baselines provided in NISTIRs 8259A and 8259B and explains how to integrate those baselines with organization- or application-specific requirements (e.g., industry standards, regulatory guidance) to develop a IoT cybersecurity profile suitable for specific IoT device customers or applications. The process in NISTIR 8259C guides organizations needing to define a more detailed set of capabilities responding to the concerns of a specific sector, based on some authoritative source such as a standard or other guidance, and could be used by organizations seeking to procure IoT technology or by manufacturers looking to match their products to customer requirements.

- **Draft NISTIR 8259D**, ***Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government***, provides a worked example result of applying the NISTIR 8259C process, focused on the federal government customer space, where the requirements of the FISMA process and the SP 800-53 security and privacy controls catalogue are the essential guidance. NISTIR 8259D provides a device-centric, cybersecurity-oriented profile of the NISTIR 8259A and 8259B core baselines, calibrated against the FISMA low baseline described in NIST SP 800-53B as an example of the criteria for minimal securability for federal use cases.

Noting that ETSI EN 303 645 security standard intends to**prepare the consumer IoT devices to be protected against the most common cybersecurity threats**. To do so, it contains a set of security and privacy requirements and recommendations that manufacturers shall implement in their products. These specifications cover different areas and are divided into 13 categories:

1. No universal default passwords.
2. Implement a means to manage reports of vulnerabilities.
3. Keep software updated.
4. Securely store sensitive security parameters.
5. Communicate securely.
6. Minimize exposed attack surfaces.
7. Ensure software integrity.
8. Ensure that personal data is secure.

9. Make systems resilient to outages.
10. Examine system telemetry data.
11. Make it easy for users to delete personal data.
12. Make installation and maintenance of devices easy.
13. Validate input data.

Additionally, the ETSI EN 303 645 standard also includes a **data protection provision** to help manufacturers to provide a number of features in the IoT devices **to protect users' personal data**, like for example give consumers clear and transparent information about what personal data are processed, how it is being used, by whom, and for what purposes, for each device and service. These requirements can also help to comply with privacy requirements (e.g: General Data Protection Regulation (GDPR)).

Given these characteristics the choice of ETSI EN 303 645, without examining it relationship to other relevant standards, would not be appropriate. An indicative list of standards is attached as a appendix.

Question 13: [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard? Question 14: 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?

No response recorded by FASE

Question 15: 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?

Government should review all relevant standards and develop a performance and outcome guide that refences the best practice across all relevant standard regimes.

Question 16: What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Consumers need to awareness and education to understand the risk and the levels of controls that they desire for their own requirements.

Question 17: Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not? Question 18: Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?

Informed choice is the overriding principle here and government should support actions to ensure this outcome.

Such a scheme will be more complex than kilojoule food labelling and power ratings. It may be possible to identify a 32 to 5 criteria like Quality ticks rated on a scale for each criterion that is easily understood and also could be supported business as it is a selling point.

a. If so, which existing labelling scheme should Australia seek to follow?

No opinion this point.

Question 19: Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

They should be treated like any device or software and vulnerabilities are addressed when the arise if not apparent or existing at manufacture.

Question 20: Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

No response recorded by FASE**.**

Question 21: Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Yes, it will assist in supporting informed choice.

Question 22: Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?
Voluntary guidance preferred as there is a lesser impact on already stretched business accountability.

Question 23: 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?
A no cost, volunteer, regular security health and hygiene check program would be a useful initiative. Such a scheme would allow business to have some independent verification of partners and suppliers' security status.

Question 24: Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

No response recorded by FASE.

Question 25: If there anything else we should consider in the design of a health check program?
Just like business value and assurance to customers is advantaged by a Quality System recognition, an effective program would be of value to business and stakeholders, including supply chain partners. It should include other security disciplines such as done in the DISP membership accreditation.

Following questions where not responded to as they are outside FASE's scope of activities.

Question 26: What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?
No response recorded by FASE.

Question 27: 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?
No response recorded by FASE.

Question 28: What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

No response recorded by FASE.

Conclusion

FASE has made some specific recommendations and included specific comments in the text that provide suggestion for action. Members of FASE are available for further consultation on any of the issues raised on to provide additional information on the topic

FASE Executive

Chair Nicholas Martin (AGL) [redacted]
Deputy Chair Policy Jason Brown (Thales) [redacted]
Deputy Chair Operations John Yates (Scentregroup) [redacted]
Secretariat Melanie Power (Virgin Australia) [redacted]

Appendix A

Relevant ISI/IEC standards

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62443 (all parts), *Security for industrial automation and control systems*

ISO/IEC 15045 (all parts), *Home electronic system (HES) gateway*

ISO/IEC 24748 and ISO/IEC/IEEE 24748, *Systems and software engineering — Life cycle management*

ISO/IEC 24767 (all parts), *Information technology — Home network security*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*

ISO/IEC 27034 (all parts), *Information technology — Security techniques — Application security*

ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information security incident management*

ISO/IEC 27040, *Information technology — Security techniques — Storage security*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

ISO/IEC/IEEE 8802-11:2012/Amd.2:2014, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications AMENDMENT 2: MAC enhancements for robust audio video streaming (adoption of IEEE Std 802.11aa-2012)*

ISO/IEC/IEEE 8802-15-4, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)*

ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

ISO/IEC/IEEE 24765, *Systems and software engineering — Vocabulary*

ISO/IEC/IEEE 42010, *Systems and software engineering — Architecture description*

ISO 10795:2011, *Space systems — Programme management and quality — Vocabulary*

ISO 31000, *Risk management — Guidelines*

ISO 31010, *Risk management — Risk assessment techniques*

BS 10012, *Personal Information Management System*

NISTIR 7628, *Guidelines for Smart Grid Cybersecurity*

NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*

NIST SP 1500-201, *Framework for Cyber-Physical Systems*

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*

NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*