Australian Government

Department of Home Affairs

Mandatory security standards and industry-led voluntary cyber security labelling scheme for consumer-grade smart devices

Impact Analysis (OIA23-05027; legacy: 23882)

Authorised Version Supplementary Explanatory Statement registered 27/03/2025 to F2025L00276

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT

2616 P - 23-02503-c

Contents

The problem

The cyber security threat environment is worsening. The COVID-19 pandemic emphasised Australia's dependence on the internet, which has generated more opportunities for malicious cyber actors to exploit vulnerable targets in Australia. The availability of simple, low-cost cybercrime tools on the dark web has made it easier to commit cyber attacks. Threat actors of all levels of sophistication are exploiting vulnerabilities in Australia's networks and smart devices.

The Department of Home Affairs (the Department) desktop research showed that households and all types of businesses are exposed to cyber security threats. Evidence suggests that malicious actors target businesses and individuals who have not implemented basic cyber security measures (regardless of size of the business or the value of data held), and are constantly scanning network services to build a list of future potential vulnerabilities.

As our economy grows increasingly connected, a growing number of households and businesses are exposed to cyber risk through supply chains. Data from the European Union shows that cyber supply chain attacks are increasing in frequency and likely to quadruple between 2020 and 2021.[1] Recent high profile cyber incidents demonstrate the wide-ranging impacts of supply chain attacks across the economy. For example, up to 1,500 businesses globally were disrupted following an attack on Kaseya, an American IT solutions provider in their supply chain.

Some indicators show that the number of cyber security incidents is increasing

Over the 2020–21 financial year, the ACSC received over 67,500 cybercrime reports, an increase of nearly 13 per cent from the previous financial year.[2] This also represented a 37 per cent increase over 2017 figures (49,238 cybercrime reports). Data from IDCARE (a non-government organisation) shows that demand for cyber security support services increased by 75 per cent between October 2019 and October 2020, suggesting a growing threat environment that is often not reported to authorities.[3] In 2016–17, official statistics showed that 9 per cent of home internet users had experienced damage or loss caused by a virus or other computer infection.[4]

However, survey data can provide conflicting indications about the growth of cyber security incidents in Australia. Australian Bureau of Statistics data records that the proportion of businesses that reported internet security incidents or breaches is falling: 8 per cent in 2019–20, compared with 11 per cent in 2017-18 and 16 per cent in 2015–16.[5] In contrast, surveys such as Ai Group's CEO Survey of Business Prospects shows that a much higher proportion of Australian businesses are being impacted - 32 per cent of Australian businesses in 2018.[6] The reason for divergent survey data is unclear but could indicate that survey participants are uncomfortable or unable to accurately answer questions given the sensitive nature of cyber security incidents.

1. ENISA 2021, Understanding the increase in supply chain security attacks.
2. Australian Cyber Security Centre 2021, ACSC Annual Cyber Threat Report.
3. IDCARE 2021, Submission to the Commonwealth Government's 2020 Privacy Act Review.
4. ABS 2018, Household use of information technology survey.
5. Australian Bureau of Statistics 2021, Characteristics of Australian Business.
6. Ai Group submission to the 2020 Cyber Security Strategy.

Cyber security threats impose a significant cost to the economy

The cost of cyber incidents to the economy is significant. These costs include ransom payments, lost revenue from business interruption, business recovery costs, lost shareholder value, reputational damage and costs to the taxpayer from any government support and assistance. Beyond the direct economic costs, there are a range of social and psychological impacts that are difficult to quantify.

Private sector estimates of total societal costs are as high as $29 billion per year (or 1.9 per cent of GDP),[7] but there can be wide variation in estimates due to limited data and generally small sample sizes. The Australian Institute of Criminology assesses that individuals suffered $1.9 billion in direct financial losses as a result of cybercrime in 2019.[8] Self-reported financial losses to the ACSC as a result of cybercrime were $33 billion in 2020-21.[9] While a significant proportion of this cost estimate can be attributed to fraud and cyber-enabled crime, this only represents a part of the problem because not all incidents are reported, and victims don't always tell authorities the cost.

Cyber security is a key business risk

In public consultation, stakeholders almost unanimously agreed that cyber security incidents are a significant business risk. Many submissions argued that the rapidly evolving nature makes it challenging for businesses to flexibly respond by identifying and implementing appropriate cyber risk mitigations.[10]

Many stakeholders acknowledged the growing threat of ransomware as a particular concern. According to the ACSC, ransomware is currently the highest cyber security threat as it requires minimal technical expertise, is low cost and can result in significant impacts to a business. In the last year, several large corporations have been impacted by ransomware attacks including Nine Entertainment (March 2021) and JBS Foods USA (June 2021). The Minister for Home Affairs' Industry Advisory Committee noted that ransomware has become one of the most immediate, highest impact cyber threats to Australia.[11]

Currently, there is no legislation mandating standards for the security of smart devices. In September 2020, the government launched the voluntary, industry-led Code of Practice: Securing the Internet of Things for Consumers (Code of Practice). This has proven to be ineffective at enhancing consumer Internet of Things (IoT) security. The Department's manufacturer research undertaken in March 2021 found that industry response to the Code of Practice was limited. This is consistent with analysis from the UK which found that their Code of Practice for Consumer IoT Security, which was released in October 2018, did not have sufficient uptake.[12] Therefore, to enhance the cyber security of smart devices, government intervention is needed.

7. Frost and Sullivan 2018, Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World.
8. Australian Institute of Criminology 2021, Estimating the pure cost of cybercrime to Australian individuals.
9. ACSC 2021, ACSC Annual Threat Report.
10. Australian Industry Group; Cisco; AIA; Charles Sturt University; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
11. Industry Advisory Committee 2021, Locked Out: Tackling Australia's ransomware threat.
12. UK Department for Digital, Culture, Media and Sport 2020, Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.

Why Government intervention is required

The Australian Government's objective is to provide confidence to end users that the digital products and services they rely on are safe. Through the 2023-2030 Australian Cyber Security Strategy, the Australian Government will take a balance of voluntary and mandatory actions to enhance the security of digital products and software without hindering innovation to achieve this objective. These measures will establish an assurance that smart devices sold in the Australian market are secure by design and by default, while also empowering consumers to make informed decisions. This will encourage changes in practice, as while smart device labelling will be voluntary, consumer preference for secure products will act as an incentive for manufacturers to adopt the labelling scheme. As a result, by 2030, there will be a significant reduction in the number of insecure smart devices available in the Australian market.

Market failures are a barrier to cyber security investment in some circumstances. In previous consultation, the Department suggested that two market failures — negative externalities and information asymmetries — impeded businesses from appropriately assessing and managing cyber security risk.

Many stakeholders supported the arguments that negative externalities and information asymmetries create a need for government action. Some stakeholders claimed that market failures were endemic within cyber security, including with respect to consumer devices.[13] For example, Kaspersky suggested that a 'typical CEO would likely decide to optimise production and product-support costs; come up with new, attractive features; and have consumers change products faster' rather than investing in cyber security. The Internet of Things Alliance Australia (IoTAA) said that device vendors don't always make the right investments in cyber security because of weak commercial incentives. The Australasian Cyber Law Institute argued that the free market does not incentivise organisations to protect personal information.[14] The Cyber Security Cooperative Research Centre argued that supply chain risk was a significant negative externality that needed to be addressed.[15]

Equally, other stakeholders contested this perspective and argued that it is in the best interests of all businesses to ensure they are cyber secure.[16] Submissions that suggested that market forces could resolve current barriers to cyber security uplift argued that attendant reputational and financial risks from cyber security incidents were sufficient for businesses to invest in cyber security.[17]

The Department concludes that market failures in the consumer smart device market are significant and enduring, warranting Australian Government intervention. In that market, stakeholder feedback supports the view that competition is primarily based on new features and cost, at the expense of cyber security.[18] In this area, information asymmetries prevent consumers from being able to make informed choices, and a negative externality occurs when risk is subsequently passed down to consumers. In the Department's view, the limited success of voluntary best- practice guidance both in Australia and internationally indicates that these challenges are unlikely to improve to an appropriate level without government intervention.

The outcomes of this report account for varying market outcomes and prioritise flexible policies that empower industry to manage risk based on an informed understanding of the threat profile and best interests of the business. It is likely that governments around the world will continue to monitor technology markets for enduring market failures in the future.

13. Office of the Victorian Information Commissioner; Law Institute of Victoria.
14. Australasian Cyber Law Institute.
15. Cyber Security Cooperative Research Centre.
16. Telstra, Communications Alliance and the Australian Mobile Telecommunications Association, Ai Group.
17. Telstra, Ai Group.
18. Cisco; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.

The current regulatory framework is complex and lacks clarity

The majority of submissions that commented on the current regulatory framework argued that current cyber security regulations are complex and create uncertainty for businesses. The Information Technology Industry Council said that 'there is a disparate array of legislation and policy related to cyber security'.[19] Kaspersky noted that the current regulatory framework 'creates a difficulty for businesses to navigate through… and identify all necessary pieces they have to be aware of'.[20] Some submissions also noted the regulatory framework is particularly unclear for small businesses who lack the capability to understand and engage with multiple pieces of legislation.[21]

Targeted regulation can support whole-of-economy cyber security uplift

Submissions generally supported the Australian Government's use of a mix of sector-specific and cross-sectoral legislation to regulate cyber security.[22] Some submissions noted that regulation should be targeted towards specific entities to support secure-by-design and to encourage broader whole-of-economy cyber security uplift while limiting regulatory burden.[23] There were mixed views on which entities should be targeted, with possible suggestions including system manufacturers, software as a service providers[24] and hardware providers.[25] Submissions generally agreed that a risk-tiering model would be appropriate to target cyber security obligations based on the sensitivity of data held by organisations.[26]

Enhanced enforcement of existing requirements can drive cyber security improvements

Some submissions noted that existing cyber security requirements could be enhanced through increased resourcing for regulators, particularly the Office of the Australian Information Commissioner (OAIC). The Australian Information Security Association encouraged the Australian Government to 'provide regulators responsible under the Privacy Act with resources required to perform their regulatory functions diligently and competently'.[27] The Office of the Victorian Information Commissioner concurred, stating that 'the OAIC would require significantly more staff and resources to enable it to carry out any new functions and responsibilities'.[28]

Other submissions considered the utility of clarifying regulator roles and responsibilities, including by designating a lead cyber security regulator.[29] The Australasian Cyber Law Institute noted that the complex legal environment resulted in a lack of clear jurisdiction for regulators supporting consumers seeking redress.[30] Wipro recommended that centralising enforcement functions 'would provide the scale to justify the investments required to be effective'.[31]

Effective enforcement of existing requirements was considered to be a possible driver for cyber security uplift, creating clear regulatory incentives for businesses to take action. Submissions generally favoured voluntary approaches over regulatory enforcement.[32]

19. Information Technology Industry Council.
20. Kaspersky.
21. Council of Small Business Organisations Australia; Ignite.
22. CSIRO; Australian Banking Association.
23. Law Institute of Victoria; Australasian Cyber Law Institute.
24. Vaultron Technology.
25. VeroGuard.
26. Vaultron Technology; Australian Banking Association; Australasian Cyber Law Institute.
27. Australian Information Security Association.
28. Office of the Victorian Information Commissioner.
29. Office of the Victorian Information Commissioner; Australasian Cyber Law Institute; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
30. Australasian Cyber Law Institute.
31. Wipro.
32. National Retail Association; National Retail Association; Telstra; IoT Alliance Australia.

What policy options are being considered?

Status quo

Retaining the status quo would see Australia maintain a voluntary and market-driven approach to smart device security. The existing Code of Practice would be relied upon to drive cyber security outcomes. A recent report by the IoT Security Foundation found that 78.4 per cent of smart device manufacturers do not have a readily detectable vulnerability disclosure policy, which is a high priority recommendation of the European Telecommunication Standards Institute (ETSI) Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645).[33] Without additional incentives, the market is likely to continue to be driven by cost rather than cyber security. In the status quo, many smart devices will continue to be sold without basic cyber security. According to current estimates, there could be as many as 371 million smart devices operating in Australia by 2024[34] and 75 billion globally by 2025.[35] As smart devices continue to grow in popularity, malicious actors will have access to more attack surfaces and vulnerabilities and will be increasingly attractive targets, particularly if personal and sensitive data can be accessed. This is likely to lead to continued negative impacts on cyber security, privacy and online safety and could lead to compromises of larger networks that devices are connected to, potentially resulting in impacts on national security.

Mandatory Standards

Providing standards for smart devices will place responsibility for ensuring that products meet baseline cyber security requirements on manufacturers and developers. This will mitigate negative externalities in the smart device market as consumers will be less likely to unknowingly purchase and bear responsibility for the consequences of an insecure smart device. Under this approach, the Australian Government must balance the mandated cyber security standards with the regulatory and economic burden on industry.

In March 2021, the Australian Government completed research on how industry responded to the voluntary Code of Practice: Securing the Internet of Things for Consumers (Code of Practice) released in September 2020. Major manufacturers said that voluntary, principles-based guidance has a limited impact on business decision-making and that they would prefer Australia to point to internationally-aligned standards. While major brands had good intentions to implement strong cyber security, the Department was able to identify some high priority, low-cost parts of the Code of Practice that had not been implemented consistently. It was difficult to engage low-cost manufacturers in this research, which suggests that voluntary guidance is likely to have had less impact on that part of the market.

Following this research, feedback was sought on whether a mandatory standard would be the best way to uplift the cyber security of smart devices. To ensure international consistency and adoption of best practice, the Department suggested that Australia consider adopting part or all of the ETSI EN 303 645.

33. IoT Security Foundation 2021, The Contemporary Use of Vulnerability Disclosure in IoT.
34. Telsyte 2020, IOT@HOME gathers pace with home-bound Australians.
35. Centre for Strategy & Evaluation Services 2020, Framing the nature and scale of cyber security vulnerabilities within the current consumer. Internet of Things (IoT) landscape.

Voluntary Labelling Scheme

The Department's analysis is that consumers do not currently have the tools to easily understand whether smart devices are cyber secure as there is often a lack of clear, accessible information available to them. A voluntary cyber security labelling scheme will provide additional guidance for consumers to inform their smart device purchase decisions. This will help to mitigate against information asymmetries that currently exist in the smart device market, as cyber security information will become more easily accessible and understandable for consumers. Research conducted by the Behavioural Economics Team of the Australian Government (BETA) showed that Australian consumers would be up to 18.8 percentage points more likely to choose a device with a cyber security label than a device with no label.

The Department asked if a cyber security labelling scheme would address this gap and encourage consumers to purchase secure smart devices. Two label designs were put forward: a voluntary star rating, similar to Singapore's labelling scheme, and a low-cost mandatory 'expiry date' label which would show the length of time that software updates will be provided. The Department also asked stakeholders whether mobile phones should be included within the scope of a labelling scheme and whether a combination of labelling and standards for smart devices would be a practical and effective approach.

BETA identified that care would need to be given to the design of the label to ensure that it is correctly interpreted by consumers. The scheme will build off international best-practice models to ensure that these limitations are appropriately mitigated.

Multi-criteria analysis

In addition to seeking feedback from stakeholders, the Department conducted a multi-criteria analysis to assess the costs and benefits of introducing a mandatory standard and a voluntary labelling scheme, compared to retaining the status quo. This involved assessing the cyber security impact, costs to industry and government, and possibility of unintended consequences of each policy, as well as the flexibility and responsiveness of each policy. An overview of the outcomes from this analysis are in the table below, including the ratings for each category.

Option	Cyber security impact	Regulatory costs to industry	Regulatory costs to Government	Flexibility and responsiveness	Potential unintended consequences	Overall rating
Status quo	No change	No change	No change	No change	No change	**0**
Mandatory standard	Very high positive impact	Medium impact	Medium impact	High positive impact	Medium potential impact	**14.5**
Voluntary labelling scheme	Low positive impact	Low negative impact	Low negative impact	High positive impact	Low negative potential	**13.5**
Mandatory labelling scheme	High positive impact	Medium impact	Medium impact	High positive impact	High negative potential	**11.5**
Mandatory standard + voluntary labelling scheme	Very high positive impact	Medium impact	Medium impact	High positive impact	Medium potential impact	**14.5**

Methodology

The following steps were undertaken for the multi-criteria analysis:

1.	Identifying the key impact categories, assessment criteria and weightings for each key impact category.
2.	Identifying individuals or groups who are likely to be affected by the policy options.
3.	Defining the assessment period.
4.	Assessing the policy options against the chosen categories and criteria.

Alt Text: Table outlining the four steps taken for the multi-criteria analysis.

For each policy option, key impact categories and assessment criteria were chosen based on the factors that the Department believes most important to decision-making. These categories and criteria were used to compare the qualitative and quantitative costs and benefits of each of the options.

To allow for comparison between the options, each policy was given rating which was made up of individual ratings from each impact category. A six-point rating scale was used, based on how well the policy addressed the assessment criteria of each impact category, where one was a very low positive impact and five was a very high positive impact (see table below). Impact ratings were weighted based on the relative importance of each category to decision-making. The status quo was used as the baseline for comparison, represented as a rating of zero for each category.

Rating	0	1	2	3	4	5
Impact	No change	Very low positive/very high negative	Low positive/ high negative	Medium	High positive/ low negative	Very high positive/very low negative

The Department also identified the groups which are most likely to be affected by the policy options to allow us to fully consider the impacts of each policy. Each policy was assessed against a period of 10 years. The table below details the key aspects of the multi-criteria analysis that were used to assess the costs and benefits of a product standard and labelling scheme.

Impact category (and reasoning)	Weighting	Assessment criteria		Affected individuals and groups
Cyber security impact Secure smart devices are key to protecting the security, privacy and safety of individuals, and to ensuring a prosperous and secure digital economy.	High	**Product standard** • Reduces the likelihood of cyber security incidents involving smart devices. • Allows for timely implementation.	**Labelling scheme** • Sufficient uptake by industry. • Results in an increased number of consumers purchasing more cyber secure products. • Results in improved consumer understanding of cyber security risks. • Allows for timely implementation.	• Users of smart devices • General public

Impact category (and reasoning)	Weighting	Assessment criteria	Affected individuals and groups
Regulatory costs to industry A product standard and labelling scheme would have costs to industry. These costs need to be proportionate to the benefits.	High	• Results in low upfront and ongoing compliance, administrative and delay costs. This may include: – Costs of implementing technical controls for manufacturers. – Cost of labelling products for manufacturers. – Assessment costs for manufacturers. – Familiarisation costs for manufacturers and retailers. – Costs of monitoring incoming stock for retailers. • Provides clear and consistent regulatory expectations to industry about roles and responsibilities. • Supports an approach that is consistent with international requirements.	• Manufacturers • Retailers
Regulatory costs to Government A product standard and labelling scheme would have costs to Government. These costs need to be proportionate to the benefits.	High	• Minimises upfront structural, organisational and regulatory change to implement, including minimal impact on existing processes and minimal regulatory layers. • Supports efficient ongoing administrative processes. • Clearly defines appropriate roles and responsibilities.	• Australian Government
Flexibility and responsiveness Smart technologies and the cyber security threat environment are still evolving. Any regulation needs to be sufficiently flexible to allow for these developments.	Medium	• Allows flexibility for industry by minimising prescriptive requirements, remaining technology-neutral and allowing innovative solutions. • Allows flexibility for government in addressing emerging security risks. • Allows for timely transition as international approaches evolve.	• Users of smart devices • Manufacturers • Retailers • Australian Government
Potential unintended consequences A product standard and labelling scheme may have unintended consequences. The risk of unintended consequences should be minimised.	Medium	• Results in minimal additional costs passed to consumers. • Results in minimal impacts on product availability. • Results in minimal impacts on competition. • Can be appropriately enforced.	• Users of smart devices • Manufacturers • Retailers • Australian Government

What is the likely net benefit of each option

Comparison of options

Option	Cyber Security Impact	Regulatory Costs to industry	Regulatory Costs to Government	Flexibility and responsiveness	Potential unintended consequences	Overall rating
Status quo	0	0	0	0	0	0
Mandatory standard	5	3	3	2	1.5	14.5
Voluntary labelling scheme	1.5	4	4	2	2	13.5
Mandatory Labelling scheme	4	3	3	2	0.5	11.5
Mandatory standard and voluntary labelling scheme	5	3	3	2	1.5	14.5

Mandatory Standards

Impact category	Assessment data	Rating	Weighting	Overall rating
Cyber security impact	• The UK modelled that the probability of attacks on smart devices could be reduced by between 20 and 70 per cent through a standard consisting of the first three principles of ETSI EN 303 645.[36] • This aligns with technical advice from the Australian Cyber Security Centre that the first three principles of ETSI EN 303 645 are the highest priority technical controls.[37] • The precise frequency and cost of IoT-based incidents is unknown, but there is sufficient evidence to demonstrate that the costs are significant. – The UK estimates that 5 per cent of smart devices will be exploited each year.[38] – ABS data shows that 8 per cent of businesses in 2019-20[39] and 9 per cent of home internet users in 2016-17 experienced a cyber security incident.[40] – The average reported loss from a cybercrime incident to the Australian Cyber Security Centre is appropriately $9,000 for a small business, $33,000 for a medium business and $19,000 for a large organisation.[41] There are a number of limitations to these estimates and they should be only be considered indicative. However, it does demonstrate that the cost of a cyber security incident is likely to be much larger than the cost of implementing technical controls on a smart device. – There are also other difficult to quantify impacts from cyber security incidents, such as emotional distress and loss of privacy. • As a mandatory requirement, a standard would have a relatively rapid impact on the market, accounting for the time needed to pass legislation and an appropriate phased introduction for manufacturers and retailers. • The cyber security impact of a mandatory standard is assessed to have a **VERY HIGH POSITIVE IMPACT (5).**	5	100 %	5

36. UK DCMS 2019, Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment.
37. Australian Government 2020, Code of Practice: Securing the Internet of Things for Consumers.
38. UK DCMS 2019, Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment.
39. ABS 2018, Household use of information technology survey.
40. Australian Bureau of Statistics 2021, Characteristics of Australian Business.
41. Australian Cyber Security Centre 2021, ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021.

Impact category	Assessment data	Rating	Weighting	Overall rating
Regulatory costs to industry	**Manufacturers** • An initial one-off cost of 0.28 per cent of turnover from sales of smart devices and an annual ongoing cost of 0.30 per cent.[42] The Department estimates this will equate to an approximate cost of $46.3 million over 10 years (2021 dollars). • Regulatory costs would be reduced through alignment with international approaches. The UK, Singapore, California and Oregon have, or are in the process of, introducing cyber security requirements for manufacturers of smart devices.[43] A number of other US states have been considering introducing legislation similar to California and Oregon[44] and the European Union have indicated that they are considering a regulatory approach to smart devices.[45] **Retailers** • One-off implementation cost of around $3.2 million. This estimate incorporates costs for familiarisation, communicating the new requirements to suppliers and updating systems to record manufacturer compliance information **Online marketplaces** • Nil - based on stakeholder feedback, enforcement of a standard by online marketplaces would occur on a voluntarily basis. • The Department has estimated that the total regulatory cost for industry will be $7.8 million in the first year, and an ongoing annual cost of $4.6 million in subsequent years (2021 base). This is a small percentage of the total value of the smart device market, estimated to be $2.5 billion annually (2021 base). • The regulatory costs to industry of a mandatory standard are assessed to have a **MEDIUM IMPACT (3)**.	3	100 %	3
Regulatory costs to Government	• Approximately $5 million over 4 years. This includes costs for education, market surveillance and enforcement. • Use of an existing regulator would maximise regulatory efficiency by utilising existing organisational and administrative processes. • The regulatory costs to Government of a mandatory standard are assessed to have a **MEDIUM IMPACT (3).**	3	100 %	3

42. These have been figures updated since our call for views to reflect stakeholder feedback. The Department's initial estimate included costs for disposal of non-compliant stock. However, a standard would include a period for gradual implementation to allow for the sale of older stock. Based on estimates from UK DCMS 2020, Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
43. UK Department for Digital, Culture, Media and Sport 2021, New cyber security laws to protect smart devices amid pandemic sales surge; Cyber Security Agency of Singapore 2021, Cybersecurity Labelling Scheme (CLS); SB-327 Information privacy: connected devices; House Bill 2395.
44. Government Technology 2019, State Lawmakers Go After IoT Security Risks (Contributed).
45. Council of the European Union 2020, Council Conclusions on the cybersecurity of connected devices.

Impact category	Assessment data	Rating	Weighting	Overall rating
Flexibility and responsiveness	• Maintenance of standards to account for evolving technology and the developing needs of the market is a core part of ETSI's model. According to ETSI, 'standards are updated as required to take account of the latest developments and revised versions are published'.[46] • Software patching and vulnerability disclosure policies will continue to be an enduring part of cyber security best-practice, so this part of the standard is unlikely to require updating for the foreseeable future. • The flexibility and responsiveness of a mandatory standard is assessed to have a **HIGH POSITIVE IMPACT (4).**	4	50%	2

46. ETSI, Standards making.

Voluntary Labelling Scheme

Impact category	Assessment data	Rating	Weighting	Overall rating
Cyber security impact	• Research conducted by BETA showed that Australian consumers would respond positively to a star rating cyber security label. – Participants in this study were 18.8 percentage points more likely to choose a device with a star rating label than a device with no label. This is consistent with existing international data[47] and stakeholder feedback which generally preferred a star rating label. – 83 per cent of participants at least somewhat agreed that they would use a cyber security label to help them when shopping for smart devices. – The study found that consumers were more likely to misunderstand the meaning of a star rating label compared to other labels. However, this could be mitigated and addressed through education and awareness-raising. – Over time, a label is likely to improve consumers' awareness and understanding of cyber security.[48] • Uptake of a voluntary scheme and impact on the market would likely take time and concerted promotion to be fully realised over the first ten years. – Some stakeholders felt that a voluntary label is unlikely to achieve sufficient scale, particularly in the lowest-cost part of the market, which presents the most cyber security risk. – Other stakeholder feedback indicated that as consumers begin to make purchasing decisions based on cyber security, manufacturers may be incentivised to invest in cyber security and use the label as a way to compete in the market. – Participation could be encouraged through alignment with international schemes. Available data on the Singapore Government's voluntary labelling scheme shows that the scheme is growing and 61 devices have been labelled in its first 12 months of operation.[49]	1.5	100 %	1.5

47. Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong 2020, The impact of IoT security labelling on consumer product choice and willingness to pay.
48. UK DCMS 2019, Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment.
49. Cyber Security Agency of Singapore 2021, Cybersecurity Labelling Scheme Product List.

Impact category	Assessment data	Rating	Weighting	Overall rating
Cyber security impact *continued*	• Further consultation would be required before a voluntary scheme could be implemented. This would include co-design of the scheme with industry and appointment of an administration body to oversee the scheme. • Due to the time required to achieve sufficient scale, the cyber security impact of a voluntary labelling scheme is assessed to have a **LOW POSITIVE IMPACT (1.5).**			
Regulatory costs to industry	**Manufacturers** • As a voluntary measure, businesses would only label their smart products if the benefits outweigh the costs. • For businesses that choose to participate, there would likely be testing and/or self-assessment costs, administration costs, product labelling and marketing costs. – Administrative costs to industry under Singapore's scheme are approximately AUD50-3,700 per device (depending on the rating level being sought). • Aligning with existing and emerging international schemes will reduce regulatory costs for industry. **Retailers and online marketplaces** • Nil • The regulatory costs to industry of a voluntary labelling scheme are assessed to have a **LOW NEGATIVE IMPACT (4).**	4	100 %	4
Regulatory costs to Government	• There may be some small costs to Government to provide initial funding to an industry-led administration body to oversee the scheme. • As the labelling scheme will be voluntary and will be led by a peak industry body, the will be no regulatory cost to Government. • The regulatory costs to Government of a voluntary labelling scheme are assessed to have a **LOW NEGATIVE IMPACT (4).**	4	100 %	4
Flexibility and responsiveness	• Retaining a voluntary approach would ensure flexibility to adapt to changes in the threat environment or emerging international approaches as it would allow an alternative to be adopted by Government in the future. • The flexibility and responsiveness of a voluntary labelling scheme is assessed to have a **HIGH POSITIVE IMPACT (4).**	4	50%	2

Impact category	Assessment data	Rating	Weighting	Overall rating
Potential unintended consequences	• Some consumers may not understand or appropriately utilise the label. Ongoing education would be required to ensure the labelling scheme is effective in influencing consumer decisions. • Businesses would only choose to participate if the benefits outweighed the costs, so it is unlikely that costs would be passed to consumers or there would be reduced product availability in the Australian market. • The administration body of the scheme would undertake appropriate auditing and approval of self-assessments. • The Australian Consumer Law would deter manufacturers from making misleading or deceptive claims about security and the Australian Competition and Consumer Commission would play an enforcement role where required. • The risk of unintended consequences of a voluntary labelling scheme is assessed to have a **LOW POTENTIAL NEGATIVE IMPACT (4).**	4	50%	2

Standards for Smart Devices

Stakeholders generally agreed that smart device security is a problem and supported the Department's analysis that the smart device market is driven by cost and consumer experience, rather than cyber security.[50] The Department was told that 'currently, manufacturers of smart devices and developers of related services lack strong incentives to invest in security features or maintain ongoing security quality after safety'.[51] Cisco said that cost plays a prominent role in the buying decisions of consumers, meaning that 'vendors with lower security, and hence generally lower cost, are often rewarded with more business'.

Voluntary Approach

There was mixed feedback about whether Australia's current voluntary approach is effective in addressing the problem. Academics and legal groups like Deakin University and UNSW Allens Hub for Technology told the Department that a voluntary approach is likely to be insufficient.[52] The Australian Competition and Consumer Commission (ACCC) said that 'markets alone cannot deliver stronger cyber security' and the Department heard that the UK's voluntary Code of Practice for Consumer IoT Security is 'significant proof of the lack of incentive provided by voluntary codes'.[53] McAfee said that 'something must be done to assure smart devices of all types, costs and complexity are properly secured'.

In contrast, industry groups such as the Communications Alliance, Australian Mobile Telecommunications Association and Digital Industry Group were more likely to think that sufficient time had not passed to assess the impact of the voluntary Code of Practice.[54] These stakeholders tended to be more supportive of increasing market incentives for adoption of existing best practice and standards.[55] Other reasons stakeholders supported retaining a voluntary approach included cost[56], lack of device manufacturing in Australia[57] and the potential for consumers to obtain a false sense of security from mandatory compliance regimes.[58] The IoTAA's submission included a proposal for a voluntary, industry-led certification and labelling scheme as an alternative to mandatory standards.

50. Internet of Things Alliance Australia; Australian Communications Consumer Action Network; Deakin University; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
51. UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
52. McAfee; Deakin University; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
53. UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
54. Australian Industry Group; Business Council of Australia; Communications Alliance and Australian Mobile Telecommunications Association; Digital Industry Group; National Retail Association.
55. Australian Strategic Policy Institute Roundtable, 18 August 2021; Internet of Things Alliance Australia; Telstra.
56. Australian Strategic Policy Institute Roundtable, 18 August 2021
57. Law Institute of Victoria.
58. Telstra.

Mandatory Approach

While the Department heard that regulations should only be used as a last resort[59] and must demonstrate a net benefit to society[60], the majority of stakeholders were supportive of introducing a mandatory standard for smart devices in Australia.[61] A mandatory standard was seen as an important way of ensuring the burden for cyber security does not disproportionately fall to consumers.[62] Some stakeholders told us that without standards, Australia risks a worsening security posture as insecure devices continue to be sold on the market.[63]

There was strong support for Australia adopting international standards because we are a small technology market.[64] Stakeholders said that aligning internationally would help reduce regulatory burden and barriers to entry in the Australian market.[65] The Department also heard that a standard would need to be future-proof to adapt to changes in the threat environment[66] and would need to be accompanied by strong enforcement to ensure compliance by industry.[67]

ETSI EN 303 645 was generally seen as the appropriate standard for consumer smart devices in Australia.[68] McAfee told us that the 'cybersecurity provisions within the standard are common sense based and needed so as not to allow an existing attack vector to continue'. Some manufacturers and retailers told us that the ETSI standard is achievable for industry.[69] Other feedback encouraged the Department to consider different standards instead of, or in combination with the ETSI standard, such as standards from the European Union Agency for Cybersecurity (ENISA), National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO).[70] Stakeholders said that a single standard or 'one-size-fits-all' approach is unlikely to address the complexity of the smart device ecosystem.[71]

Some suggested referring to multiple relevant standards as this would provide businesses who supply or source their products from multiple jurisdictions with flexibility.[72]

Of those that supported the ETSI standard, there was mixed feedback about mandating the whole standard or the first three principles identified in the call for views (no default universal passwords; vulnerability disclosure policy; keep software updated). Industry groups and manufacturers tended to be more supportive of adopting the first three initially as a way of balancing security and cost to industry.[73] The Consumer Electronic Suppliers' Association and the Air-Conditioning and Refrigeration Equipment Manufacturers Association of Australia told us that they 'consider the top three requirements of the standard to be adequate in the first instance as larger markets such as Europe and the UK have adopted or intend to adopt these higher priority principles.'

59. Smart Device Security Roundtable, 27 July 2021.
60. Consumer Electronic Suppliers' Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia.
61. IoXT Alliance; Google; ACCC; Australian Communications Consumer Action Network; McAfee; Australian Information Security Association; University of Queensland; Water Services Association of Australia; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
62. University of New South Wales Allens Hub Roundtable, 16 August 2021; ACCC; Water Services Association of Australia.
63. Smart Device Security Roundtable, 27 July 2021.
64. Industry Co-design Working Group Roundtable, 23 July 2021; Smart Device Security Roundtable, 27 July 2021; University of New South Wales Allens Hub Roundtable, 16 August 2021; McAfee; National Retail Association; Water Services Association of Australia; Palo Alto.
65. Smart Device Security Roundtable, 27 July 2021; CyberCX; Business Council of Australia; Australian Industry Group; ForgeRock; Standards Australia; Australian Information Security Association.
66. UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law; Raised at the digital open forums held during the consultation period.
67. Smart Device Security Roundtable, 27 July 2021; IoXT Alliance; ACCC; Australian Communications Consumer Action Network; Australian Information Industry Association; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
68. Internet of Things Alliance Australia; Consumer Electronic Suppliers' Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; Telstra; McAfee; Kaspersky; Palo Alto; Australian Communications Consumer Action Network; Australian Information Security Association; National Retail Association; Law Institute of Victoria; AustCyber; Water Services Association of Australia; ForgeRock.
69. Smart Device Security Roundtable, 27 July 2021.
70. Internet of Things Alliance Australia; Australian Industry Group; Telstra; Australian Information Security Association; Water Services Association of Australia.
71. Internet of Things Alliance Australia; Telstra.
72. IoXT Alliance; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
73. Consumer Electronic Suppliers' Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; Kaspersky; Australian Information Security Association; Water Services Association of Australia; Palo Alto; Communications Alliance and Australian Mobile Telecommunications Association.

In comparison, consumer advocates and some cyber security companies advocated for the adoption of the whole standard.[74] Some stakeholders told us that implementing only the first three principles would not provide sufficient protection against cyber incidents[75]. The IoXT Alliance said that while the first three 'address the most egregious issues', many important issues are not addressed and 'there is a danger that a program based on the first three will cause a large drop in consumer confidence once the first attack occurs for a device which has only met the top three'. Some argued that provisions for the protection of user data and privacy should be included in any mandatory standard.[76]

Other concerns and options

The Department heard from the Australian Information Security Association that the Australian Government would need to ensure that small and medium retailers and online marketplaces are not disproportionally affected. In reference to the role of online marketplaces, eBay told us that they would take a similar approach to product safety and would work with the Australian Government to voluntarily remove smart devices that do not comply with a mandatory standard.

Other stakeholders said that efforts to secure the network-level of smart devices should be considered because securing the device-level level has a number of challenges, such as technical limitations of some devices.[77] Palo Alto told us that the 'network is a logical detection and enforcement point for IoT security, because all IoT devices leverage mobile/ISP networks to communicate'. Other suggestions to improve the cyber security of smart devices in Australia included considering the role of internet service providers (ISPs),[78] harmonising existing standards,[79] increased awareness raising,[80] greater involvement in standards development,[81] and improving legal recourse for consumers.[82]

Labelling for Smart Devices

Our analysis is that consumers do not currently have the tools to easily understand whether smart devices are cyber secure as there is often a lack of clear, accessible information available to them. The Department asked if a cyber security labelling scheme would address this gap and encourage consumers to purchase secure smart devices. Two label designs were put forward: a voluntary star rating, similar to Singapore's labelling scheme, and a low-cost mandatory 'expiry date' label which would show the length of time that software updates will be provided. The Department also asked stakeholders whether mobile phones should be included within the scope of a labelling scheme and whether a combination of labelling and standards for smart devices would be a practical and effective approach.

Stakeholders generally agreed that consumers currently do not have the tools to easily understand whether smart devices are cyber secure due to a lack of clear and accessible information.[83] The Information Technology Industry Council told us that end-users currently have 'limited insight into the presence of security features in a finished product prior to purchase'.[84] Some stakeholders told us that labelling would improve consumer awareness of cyber security for smart devices and enable consumers to make more informed purchasing decisions.[85] We also heard that labelling could create market incentives for companies to compete on cyber security.[86]

74. IoXT Alliance; Australian Communications Consumer Action Network; McAfee; VeroGuard Systems.
75. Smart Device Security Roundtable, 27 July 2021.
76. Australian Communications Consumer Action Network; University of Queensland; ForgeRock; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
77. Cisco; Palo Alto; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law; Raised at the majority of the digital open forums held during the consultation period.
78. UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
79. Australian Industry Group; Google.
80. Communications Alliance and Australian Mobile Telecommunications Association; Digital Industry Group; Law Institute of Victoria.
81. CyberCX; Standards Australia; Australian Information Industry Association; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
82. CyberCX; Law Institute of Victoria.
83. Industry Co-design Working Group Roundtable, 23 July 2021; Telstra; Information Technology Industry Council; Raised at the digital open forums held during the consultation period.
84. 160 Information Technology Industry Council.
85. Google; Australian Competition and Consumer Commission; Innovative Research Universities; Telstra; UNSW Allens Hub for Technology/ Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
86. IoXT Alliance; Crowdstrike.

However, other stakeholders were sceptical of a labelling scheme for smart devices. eBay Australia was not supportive of a labelling scheme in Australia and instead recommended an education campaign 'with a focus on key groups and devices that create risk'.[87]

Stakeholders reported numerous limitations to labels, including:

- Difficulties in communicating complex cyber security information in a label which risks leading consumers into a false sense of security;[88]
- A static label would potentially become obsolete in a dynamic and ever-evolving cyber threat environment;[89]
- Consumers do not gain a direct financial benefit from investing in devices with higher levels of cyber security, compared to other schemes like energy and water efficiency;
- Increased costs to manufacturers and retailers which may be passed onto consumers;[90]
- Limited existing data about the effectiveness of labelling schemes in changing consumer behaviour;[91] and
- Insufficient time has passed to assess the success of international labelling schemes.[92]

Voluntary Approach

Of the stakeholders who supported a labelling scheme, there was a roughly even split between stakeholders on whether a labelling scheme should be mandatory or voluntary. Some stakeholders strongly supported the idea of a voluntary scheme as it would allow for flexibility to adapt to the threat environment without creating regulatory burden.[93] The Cyber Security Cooperative Research Centre and CyberCX thought a voluntary approach would generate greater industry buy-in and should be the first step before adopting a mandatory approach.[94]

The option of a voluntary labelling scheme was rejected by other stakeholders who felt that a voluntary label would not have sufficient industry uptake.[95] Some stakeholders noted that a company would be unlikely to label their product with a poor security rating on a voluntary basis.[96] We were told that for a voluntary scheme to be effective, it would need to have low implementation costs, international alignment and adequate consumer understanding and use of the label.[97] Some stakeholders thought that consumer demand would not be enough to drive uptake of a voluntary label[98] and others suggested the Australian Government would need to provide financial incentives.

Mandatory Approach

Other stakeholders expressed support for a mandatory approach to labelling.[99] McAfee noted that a mandatory approach would have a more immediate effect on the marketplace compared to a voluntary approach.[100] The University of Melbourne argued that a mandatory approach is justified given the large amount of personal and biometric data that smart devices now collect.[101]

However, the Department also received feedback that a mandatory approach would impose too much regulatory burden.[102] CyberCX argued that further consumer education and awareness is necessary before introducing a mandatory labelling regime.[103]

87. eBay Australia.
88. Cisco Australia; Digital Industry Group; IoTAA; Telstra; eBay.
89. Industry Co-design Working Group Roundtable, 23 July 2021; Smart Device Security Roundtable, 30 July 2021; Facebook; Queensland University of Technology; Raised at the digital open forums held during the consultation period.
90. Consumer Electronic Suppliers Association and and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; Raised at the digital open forums held during the consultation period.
91. Smart Device Security Roundtable, 27 July 2021; Facebook; Digital Industry Group.
92. Australian Industry Group; Facebook.
93. Cyber Security Cooperative Research Centre; Information Technology Industry Council; Telstra; US Chamber of Commerce; Communications Alliance and Australian Mobile Telecommunications Association.
94. 170 Cyber Security Cooperative Research Centre; CyberCX.
95. Australian Communications Consumer Action Network; Google; IoXT Alliance; ForgeRock.
96. Smart Device Security Roundtable, 27 July 2021
97. IoXT Alliance.
98. Consumer Electronic Suppliers Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; University of Melbourne; Google; Australian Communications Consumer Action Network.
99. CPA Australia; Wipro; University of Melbourne; Law Institute of Victoria; Australian Communications Consumer Action Network; University of Queensland.
100. McAfee.
101. University of Melbourne.
102. Smart Device Security Roundtable, 27 July 2021; Facebook.
103. CyberCX.

Some stakeholders noted that a mandatory scheme would need to be aligned with international jurisdictions or there would be a risk of products being taken off the Australian market.[104] The US Chamber of Commerce advised that President Biden issued an Executive Order on 12 May 2021 to develop a pilot consumer labelling program (using a graded label), which would have implications for Australia.[105]

Label Design Considerations

Star rating label

Stakeholders were more supportive of a star rating label than an expiry date label. Stakeholders who advocated for a star rating argued that consumers are already familiar with the concept of a star rating so this design would appeal to consumers.[106] The University of Melbourne said that a star rating is a simple way of communicating information and would prevent information overload and other cognitive biases.[107] In research conducted by the Australian Information Security Association, a star rating label rated highly compared to other types of labels.[108]

The main objection to this type of label was that cyber security cannot be easily translated into star ratings as there is no clear assessment framework for cyber security, compared to water or energy efficiency.[109] We also heard that because different smart devices have different security requirements, there are challenges associated with determining the appropriate security level for a device and communicating this to consumers.[110] IoXT Alliance provided the example that even though light bulbs have lower security controls than cameras, 'a 1-star lightbulb may be perfectly suited for the consumer while a 1-star camera may not'.[111] Some stakeholders noted that consumers have been taught to assume that star ratings apply throughout the life of the product, which would be misleading for smart devices where a rating may no longer be accurate if a vulnerability is found.[112] Additionally, a few stakeholders argued that discrepancies in accreditation ratings across international jurisdictions would complicate the implementation of a star rating.

Expiry date label

There was less support amongst stakeholders for an expiry date label. Stakeholders reported that because Australia's smart device market is largely supported by global offshore suppliers who are already subject to regulations of other jurisdictions, any unique requirements may have a negative impact.[113] Numerous stakeholders pointed to the challenge of pre-determining an expiry date for devices[114] and PWC argued that a standard lifespan for devices is not possible to define.[115] Additionally, stakeholders were concerned that introducing expiry dates could result in products being deemed as 'expired' and could contribute to unnecessary e-waste.[116] The IoXT Alliance recommended an end-of-life policy as an alternative.

Other stakeholders were supportive of an expiry date label as they thought it is important information for consumers to know.[117] Some stakeholders told the Department they preferred an expiry date label because it would align with the management of other products, such as operating systems.[118] Other stakeholders reported that most manufacturers already have product life cycles that define end support dates so they could provide this with a high level of assurance.[119] We heard that this type of label is reasonable provided that manufacturers are obligated to ensure patching and maintenance services throughout the product's life.

104. Australian Banking Association; Raised at the digital open forums held during the consultation period.
105. US Chamber of Commerce.
106. The University of Melbourne.
107. Innovative Research Universities.
108. Further information contained in the Australian Information Security Association's public submission.
109. Law Institute of Victoria; Telstra.
110. IoXT.
111. IoXT.
112. Smart Device Security Roundtable, 27 July 2021
113. Smart Device Security Roundtable, 27 July 2021; Consumer Electronic Suppliers Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; Australian Banking Association.
114. Smart Device Security Roundtable, 27 July 2021; Digital Industry Group; PWC; IoXT Alliance; ForgeRock; Raised at the digital open forums held during the consultation period.
115. PWC; Australian Information Security Association.
116. Smart Device Security Roundtable, 27 July 2021.
117. University of Melbourne; Fortinet.
118. Smart Device Security Roundtable, 27 July 2021
119. Smart Device Security Roundtable, 27 July 2021

Physical and digital labelling

The majority of stakeholders expressed support for a digital label rather than a physical label. Digital labels were favoured as they can be easily updated to better reflect changes in the threat environment and product's security, unlike a static physical label.[120] Digital labels were also preferred because they are lower cost[121] and can provide more detailed information, which would better inform consumers at the point of purchase. Cisco suggested that a digital label could be processed by business automation solutions, which could allow vulnerabilities to be identified and automated protections to be provided.

In contrast, physical labels were generally not supported. The Consumer Electronics Suppliers Association and the Air-Conditioning and Refrigeration Equipment Manufacturers Association of Australia pointed to difficulties in physically labelling consumer appliances that are not seen by the consumer at the point of purchase, but are directly installed, such as home energy storage systems and air conditioners.[122] As an alternative, a number of stakeholders suggested a 'live label' in the form of a QR code or URL which would link the consumer to detailed and up-to-date information online.[123]

Numerous stakeholders argued that labels should be physical and digital to cover all consumer types.[124]

Devices in scope

Many stakeholders were in favour of including mobile phones under a mandatory labelling scheme.[125] Stakeholders pointed out that mobile phones are one of the most common smart devices used by consumers[126] and pose significant security and privacy risks to consumers due to the types and volume of data they collect.[127] We were also told that mobile phones are a key source of security failures.[128]

Other stakeholders did not support including mobile phones.[129] Notable opposing views came from the Communications Alliance, Australian Mobile Telecommunications Association, Consumer Electronics Suppliers' Association and Telstra. Stakeholders submitted that mobile phones have their own security ecosystem that already incorporates 'rigorous cyber security', including regular security updates from the manufacturers.[130] Stakeholders also pointed out that applying a labelling scheme to mobile phones would be difficult in practice due to variabilities in hardware, operating system software and applications embedded across mobile phone devices.[131] Telstra expressed concern that a security label on mobile phones may 'provide a false sense of security where users assume that because the original operating system and software was certified, the device will remain certified'.[132]

Complementarity of standards and labelling

There was general support for a combination of standards and labelling for smart devices,[133] with no stakeholders explicitly opposed to this approach. The two policies were seen as complementary and stakeholders agreed with the idea in the call for views that a standard would ensure smart devices have minimum security, while a label would communicate a device's security beyond the baseline to consumers.[134]

120. Fortinet; Australasian Cyber Law Institute; IoXT Alliance; ForgeRock; Cisco Australia; Water Services Association of Australia.
121. National Retail Association.
122. Consumer Electronic Suppliers Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia.
123. Industry Co-design Working Group Roundtable, 23 July 2021; Google; PWC; McAfee; UNSW Allens Hub for Technology / Law and Innovation / IFCYBER / SECedu / Australian Society for Computers & Law.
124. Wipro; Forum of Australasian Security Executives; CPA Australia; CyberCX; IoXT Alliance; University of Queensland; McAfee; Queensland University of Technology.
125. ForgeRock; IoXT Alliance; Queensland University of Technology.
126. IoXT Alliance.
127. Queensland University of Technology.
128. University of Melbourne; PWC; Office of the Victorian Information Commissioner.
129. Internet of Things Alliance Australia; Communications Alliance and Australian Mobile Telecommunications Association; McAfee; Information Technology Industry Council; Consumer Electronic Suppliers Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia; Telstra.
130. Consumer Electronic Suppliers Association and Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia;
131. Information Technology Industry Council; Internet of Things Alliance Australia; McAfee; Telstra.
132. Telstra.
133. Australian Information Security Association; McAfee; University of Technology Sydney; University of Melbourne; Kaspersky; Fortinet; AGL; Google; Australian Communications Consumer Action Network; Cyber CX; ForgeRock.
134. AGL.

Best option

During consultation on the Strategy, industry stakeholders showed support for a combination of a mandatory product standard and voluntary labelling scheme for smart devices. The mandatory product standard will ensure that smart devices are built with minimum security, and the voluntary labelling scheme will complement the mandatory measure by communicating the security of the device through the label to help consumers make informed purchasing decisions.

Evaluation process

The Department would be responsible for implementing this recommendation. This would include legislation design, including further consultation on scope, definitions, timelines and phasing. A yet to be identified regulatory authority would administer the recommendation, as well as developing appropriate education and awareness-raising initiatives about the standard and its implementation. A post-implementation review should occur no later than two years after implementation to ensure the standard can respond to developments in technology, the threat environment and international approaches. The review should be informed by a mix of quantitative and qualitative data, including but not limited to, data gathered by the regulator through enforcement and awareness-raising activities, in-depth interviews and surveys with manufacturers and other key industry stakeholders, and open-source research on key trends in smart device security.

Mandatory Standards

Measures of Success:

- By the implementation date, no new consumer-grade smart devices will be sold in the Australian market that do not meet the mandatory cyber security standard.

Voluntary Labelling Scheme

Measures of Success:

- Conduct a consumer survey 2 years post implementation date to determine if over 35 per cent of consumer-grade smart device purchases were influenced by a cyber security label.
- Conduct a market analysis of consumer-grade IoT devices that have a cyber security label to determine update of voluntary labelling:
  - Interim target 1 (at three years) – 50 per cent of intended products have applied the voluntary labelling system by end of 2027.
  - Interim target 2 (at four years) – 60 per cent of intended products have applied the voluntary labelling system by end of 2028.
  - Final target (at five years) – 70 per cent of intended products have applied the voluntary labelling system by end of 2029.