Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com

UPGUARD SUBMISSION:
CYBERSECURITY LEGISLATIVE REFORMS

30 February 2024

Department of Home Affairs
auscyberstartegy@homeaffairs.gov.au

UpGuard appreciates the opportunity to contribute to the Australian Government's consultation on the proposed cybersecurity legislative reforms. As a leader in the field of cybersecurity, UpGuard is committed to supporting the Government's efforts to enhance the national cybersecurity posture. The proposed reforms represent a significant step forward in addressing the evolving cyber threat landscape, and UpGuard is keen to lend its expertise and innovative solutions to assist in these endeavours.

Overarching Comments

UpGuard supports the Government's plan for Australia to become a world leader in cybersecurity by 2030 and we agree with the proposed legislative reforms in the Cyber Action Plan to address gaps in the existing regulatory framework.

UpGuard also sees clear synergies with the goals set out in the Cyber Action Plan and our own philosophy as a company, where we have built a world class capability to deliver instantaneous insights into an entity's cybersecurity profile, detailing past and present vulnerabilities, and projecting potential future threats. This knowledge is pivotal for entities aiming to enhance their cybersecurity measures in anticipation of, and in alignment with, the proposed legislative changes. Similarly, for us as a nation to achieve the ambitious cybersecurity goals set by the Government will require a similar profiling of the current security posture on a much larger scale across different industries within the country.

About UpGuard

UpGuard is an Australian cybersecurity technology company, headquartered in Hobart, Australia and Mountain View, California. With a significant operational footprint in Australia, UpGuard is at the forefront of cybersecurity innovation, dedicated to enhancing the digital resilience of organisations globally. Specialising in security ratings, vulnerability assessments, and third-party risk management, UpGuard offers indispensable tools for businesses to navigate the complexities of cyber threats and gain clear visibility on the ever changing threat landscape. Our capabilities are particularly relevant in the context of the Australian Government's ambitious cybersecurity legislation aimed at making Australia a global leader in cyber security by 2030.

Our capabilities extend to providing a transparent and easily comprehensible security score for entities, directly correlating to their cybersecurity posture and any vulnerabilities within their systems, including those stemming from their supply chain and third-party network. This scoring system not only offers a clear baseline for governmental benchmarking and monitoring efforts but also provides clear visibility of the threat landscape at any point in time and ensures that improvements in security posture can be accurately measured over time in response to regulatory changes.

In our quest to share knowledge and enhance cybersecurity awareness, UpGuard collects extensive data on security postures, vulnerabilities, and breaches. This wealth of information is utilised to produce in-depth reports and articles, sharing valuable insights and learnings with the public. Notably, our annual ASX200 reports offer a detailed analysis of the cybersecurity posture of these 200 leading companies, contributing significantly to the discourse on corporate cyber resilience in Australia.

As thought leaders in the cybersecurity sector, UpGuard is expanding its team and offerings to include policy briefs addressing cyber maturity in the region, alongside quarterly reports on cybersecurity posture across different jurisdictions. This expansion aligns with our mission to secure the world's data, aiming to provide greater visibility of the threat landscape in each area we operate. By arming companies and governments with the necessary tools to understand their baseline and maintain optimal cyber health, UpGuard is committed to enhancing the digital security of organisations worldwide.

Our offering enables entities to adopt a proactive stance towards cybersecurity, continuously aware of their position within the broader threat landscape. This proactive posture, supported by UpGuard's insights, ensures that the path towards achieving the government's 2030 vision for cyber leadership is both informed and strategic.

Responses to Part 1: New Cybersecurity Legislation

Mandatory security standard for consumer-grade Internet of Things (IoT) devices

- UpGuard acknowledges the Australian Government's initiative to introduce mandatory security standards for consumer-grade Internet of Things (IoT) devices as a critical step towards enhancing national cybersecurity. Recognising the nascent state of security-by-design in technology products both locally and internationally, we support the proposal's aim to foster improvements in this area.
- UpGuard emphasises the importance of international interoperability and alignment, especially considering Australia's position as a major importer of technology products. We advocate for leveraging the ETSI EN 303 645 standard as a foundation for these reforms, aligning with international regulatory frameworks to ensure global consistency.

- We agree with the proposal to enshrine the first three principles of the ETSI standards into legislation, focusing on eliminating universal default passwords, facilitating the reporting of cyber vulnerabilities, and mandating transparency regarding the duration of security updates for smart devices.
- These measures are vital for securing IoT devices from their inception. UpGuard also supports the designation of responsible entities—including manufacturers, subcontractors, software developers, importers, and distributors—as the bearers of compliance obligations. This comprehensive approach ensures that all participants in the IoT ecosystem adhere to a unified standard, enhancing the security posture across the board.

Recommendation and proposed solutions:

- UpGuard recognises the need for clarity on the consequences and obligations associated with breaches of the proposed standards, including liability issues within supply chains. It is essential to establish clear guidance that delineates contractual warranties and other forms of liability assurance. This clarity will be crucial for entities throughout the supply chain, given Australia's status as a net importer of manufactured goods.
- To address these concerns and ensure effective implementation, a uniform and easy to understand system will be required. In this regard, UpGuard's own system could serve as a model for the Government to consider. Our products offer a sophisticated method for measuring and ensuring compliance with the mandated security standards for IoT devices. By providing a transparent and easy-to-understand security score, UpGuard can help define what constitutes a breach in terms of security standards, such as falling below a certain score rating. This scoring system could serve as a standard for measurement, allowing entities to assess their compliance with the new security requirements and identify areas for improvement proactively.

No-fault, no-liability ransomware reporting obligation

- UpGuard supports the Australian Government's initiative to introduce a no-fault, no-liability ransomware reporting obligation, recognising the importance of this measure in the broader context of enhancing national cybersecurity resilience and gaining clearer visibility on the threat landscape. Based on our comprehensive data, which involves scanning public and private entities every second, we offer unique insights into the cyber threat landscape. Notably, our analysis of incidents involving ASX200 companies reveals that ransomware attacks is the leading category of cyber incidents, accounting for 31% of overall incidents, see Fig.1. This statistic underscores the critical need for a robust reporting framework to address the ransomware threat effectively.

Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com

Recommendation and proposed solutions:

- A significant challenge with using annual revenue as a benchmark for determining which companies are required to partake in ransomware reporting is the opacity and frequent misreporting of revenue figures for private companies. A more accurate and relevant metric for understanding the vulnerability of companies to cyber threats would be to assess their attack surface area. This assessment would consider factors such as the extent of a company's internet enablement, the number of digital assets that are internet-facing, and, given that many breaches are user-based, the size of the company's employee base. Employing these criteria would offer much clearer visibility into which entities are at higher risk and therefore should be prioritised for ransomware reporting obligations, ensuring a more targeted and effective approach to enhancing cybersecurity resilience and reporting impact.
- UpGuard's comprehensive analysis of the ASX200 provides a granular view of cybersecurity postures across various sectors, highlighting not only those who are leading in cybersecurity readiness but also those who are improving or declining over time, see **Fig 2.** This chart highlights that the most improved sectors over the past two years are: Communications, Information Technology and Industrials. Worryingly, it also highlights that the only sector to have seen a drop in its security ratings is the energy sector. Interestingly, although the chart shows that the Utilities sector has improved their overall scores by 11.1 points, our correlating breach data highlighted that this sector has seen a steadily increasing number of attacks and therefore an increase of 11.1 is insufficient to improve their security posture to a satisfactory level.
- This data is invaluable for understanding the broader cyber threat landscape and identifying patterns and vulnerabilities specific to certain industries or company sizes. Leveraging this type of detailed, sector-specific cybersecurity data could offer the

Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com

government deeper insights into effective thresholds or categorisations for mandatory reporting. Such an approach would enable a more nuanced and effective regulatory framework that considers the unique risks and challenges faced by businesses of all sizes, ensuring that cybersecurity measures are inclusive and comprehensive.

- Thus, while the intention to alleviate regulatory burdens on small businesses is commendable, it is imperative to consider the broader cybersecurity ecosystem and the potential risks of creating exemptions. By using data-driven insights, policymakers can craft more informed, targeted regulations that protect all entities within the economy, regardless of their size, from the ever-evolving threat of cybercrime. This balanced approach ensures that all businesses, including small ones, are encouraged to adopt and maintain strong cybersecurity practices, thereby enhancing the overall resilience of the national economy.

‘Limited-use’ obligation

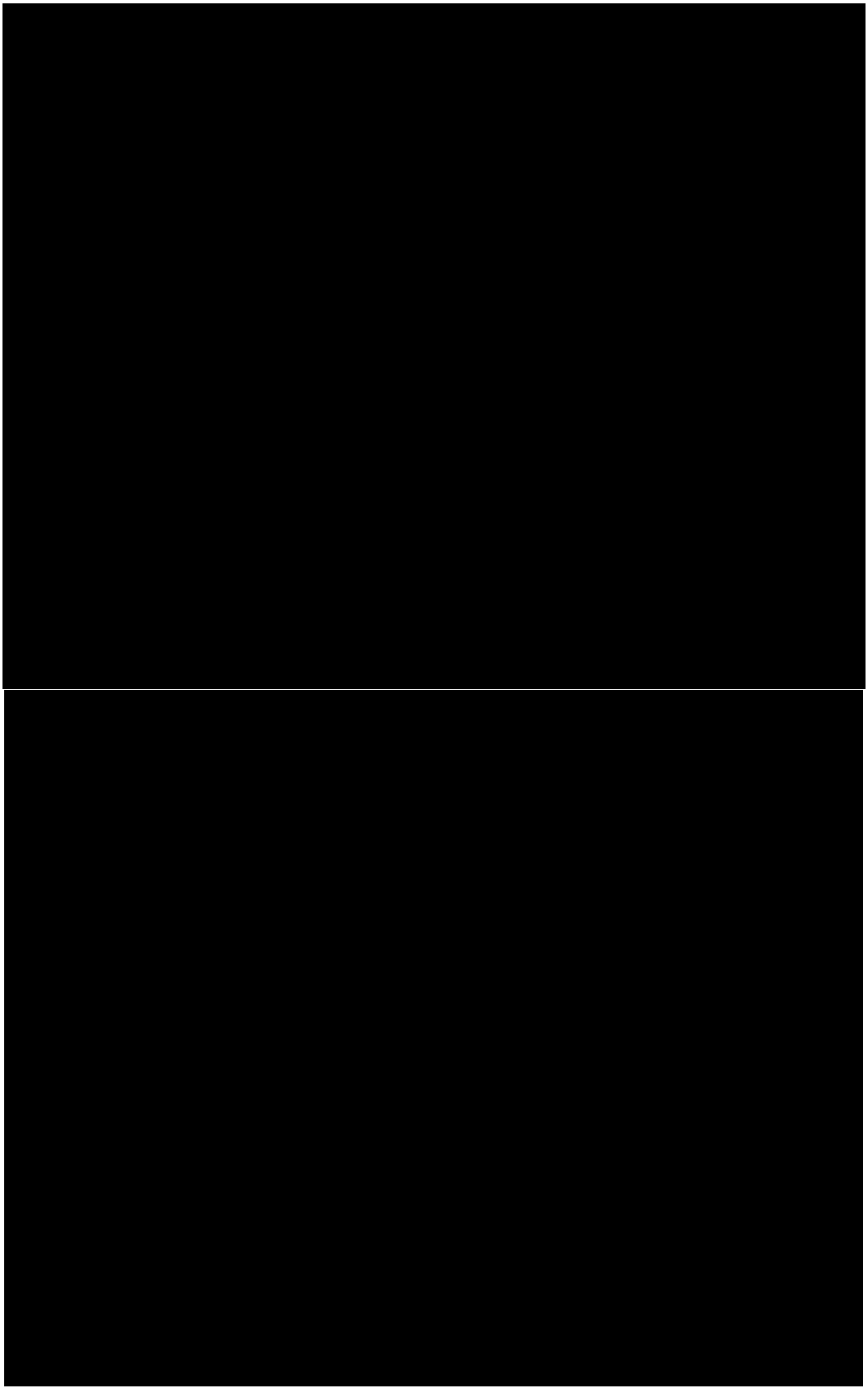
- The proposed 'limited-use' obligation has sparked legitimate concerns among industry regarding the potential for legal risks, actions, and liability associated with disclosing information to the Australian Signals Directorate (ASD). While UpGuard supports the principle of fostering enhanced information sharing to strengthen the relationship between ASD and industry, building trust is paramount. This requires a concerted effort towards transparency, genuine communication, and collaboration. There are specific

apprehensions around the purposes of informing ministers, government officials, and sharing information with other agencies for law enforcement, with fears that such disclosures could inadvertently lead to regulatory or punitive actions.

Recommendation and proposed solutions:

- UpGuard understands that the overarching intent of this obligation is to improve the cybersecurity landscape's understanding and visibility. However, given the industry's reluctance to engage with ASD, we advocate for a cybersecurity posture scoring system as a means to gain deeper insights into vulnerabilities and potential threats. Such a system could identify companies with lower security scores that are at higher risk of attacks, thereby enabling ASD to anticipate possible breaches and engage with these entities proactively, before a state of panic ensues. For example, UpGuard's ASX200 report highlights the top 10 and worst 10 performers at risk of cyber attacks **(see Fig 3 & 4)**. The top 5 sectors for reporting ransomware-related incidents in FY22-23 to ASD can be seen in **Fig 5.** Having this type of visibility on which companies are at most risk provides transparency and an opportunity for earlier engagement and collaboration.
- Addressing the concerns raised, it is crucial that disclosed information is used solely for enhancing cybersecurity, not as grounds for subsequent prosecutions. Safeguards must ensure information is not misused by law enforcement or regulatory bodies, bypassing judicial processes. Moreover, once information is disclosed, its dissemination to other organisations, departments, or the public domain must be carefully managed to prevent misinterpretation or reputational damage.
- We encourage the Government to provide clear guidelines on the non-usage of disclosed information and enhance transparency regarding the subsequent steps, including details on information sharing and briefing processes. Additionally, there should be assurances that information disclosure won't lead to undue scrutiny or legal repercussions for disclosing entities.
- In summary, while supporting the 'limited-use' obligation's concept, UpGuard emphasises the need for clear guidelines and protections to foster a secure and trust-based framework for information sharing. Through the use of a cybersecurity posture scoring system, both the industry's concerns and the goal of enhancing national cybersecurity can be addressed, enabling a proactive and collaborative approach to securing Australia's cyber future.

Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com



Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com

Establishment of a Cyber Incident Review Board

- UpGuard endorses the establishment of a Cyber Incident Review Board (CIRB), recognising the essential role such a mechanism could play in enhancing the cybersecurity landscape across Australia. We align with the position that the CIRB should adopt a no-blame approach, akin to the models used in transport and aviation safety reviews, focusing on driving continual improvement rather than attributing fault. This perspective is crucial for fostering an environment where entities are encouraged to share information about cyber incidents without fear of reprisal, thereby enriching the collective understanding and resilience against cyber threats.
- We also agree that the scope of what constitutes a 'significant cyber incident' should be broadened to encompass not only major singular events but also patterns of incidents that reflect on the broader cyber health within the economy. This approach will indeed provide a more holistic view of cybersecurity readiness and vulnerabilities, guiding where remedial actions are most urgently required.
- UpGuard sees merit in the recommendation to integrate the CIRB's review functions within the National Cyber Security Centre (NCSC), supported by an independent board. This structure could streamline efforts, reduce bureaucratic redundancy, and ensure a focused and effective incident review process. However, recognising the potential conflicts of interest and governance issues inherent in having the NCSC both coordinate across government and review incidents, we see the establishment of clear firewalls as a necessary provision to maintain the integrity and independence of reviews.

Recommendation and proposed solutions:

- UpGuard proposes that the inclusion of suitably qualified external industry voices on the CIRB or its advisory board in order to ensure there is sufficient plurality and redundancy to account for potential conflicts of interest and to cover the breadth of cyber issues that will fall within its remit. Should the government agree, UpGuard would be happy to be one of

Level 9, 45 Murray Street
Hobart TAS 7000
Australia
www.upguard.com

these industry voices, and would offer our expertise in real-time cyber threat visibility, data analysis, and the provision of actionable insights to contribute to the CIRB's objectives. Our capabilities in delivering instantaneous data and analysis, rendered comprehensible for public consumption, would enhance the board's ability to communicate its findings and recommendations effectively.

- Our data and security ratings would not only bring in-depth analytical capabilities but also ensure that the board benefits from a comprehensive and nuanced understanding of the cyber threat landscape. This could empower the CIRB to achieve its mission of improving cybersecurity practices and outcomes throughout Australia, making a substantial contribution to national security.

UpGuard would be pleased to discuss our comments, data and analysis with Home Affairs. We look forward to and support the ongoing development of the Strategy and to working closely with Home Affairs to provide innovative solutions that safeguard the digital future of the nation.

Yours sincerely,

Mary Fifita

Vice President, Corporate Development