ATLASSIAN

Atlassian’s Submission in relation to the 2023-2030 Australian Cyber Security Strategy Discussion Paper

Department of Home Affairs
auscyberstrategy@homeaffairs.gov.au

21 April 2023

We appreciate this opportunity to provide input on the further development of the 2023-2030 Australian Cyber Security Strategy (the **Strategy**) and to respond to the Discussion Paper published by the Expert Advisory Board on 27 February 2023 (the **Discussion Paper**).

At Atlassian, we build enterprise software products to help teams around the world collaborate, including for software development, project management and content management. As a digital-first company, we know the critical role that cyber security plays in ensuring the confidentiality, integrity and availability (and accordingly the privacy and trustworthiness) of our own products and services.

We also understand that this is not just an issue for one company, one sector or one country. Our entire economy is increasingly digitised, highly interconnected (including globally) and strategically targeted by malicious actors, trends that have only accelerated in recent months. Atlassian strongly supports efforts that seek to uplift cyber security capability and encourage better cyber security practices across the economy and across borders, in a way that acknowledges that responsibility for cyber security is shared by all of us.

Atlassian welcomes this consultation process and appreciates the breadth of the issues and potential proposals canvassed in the Discussion Paper. In the time since the publication of Australia’s Cyber Security Strategy 2020, the urgent and critical need to take action to ensure the security and resilience of our digital economy has been recognised by governments, businesses and societies around the world.

This means that the Discussion Paper and its proposals come at a time when multiple governments and regulators are seeking to address many of the same complex issues, including by considering appropriate cyber security standards and expectations.

Key principles to inform this consultation process

Given this current landscape, we therefore strongly believe that the Australian Government’s reforms should be considered and formulated by reference to clear guiding principles.

In late 2020, Atlassian published eight Principles for Sound Tech Policy.[1] These Principles are intended to not only guide Atlassian’s own engagement on important matters of public policy, but to set forth guiding principles for what we believe sound technology-related public policy should look like more broadly.

In line with these Principles, we believe that the Strategy, and its treatment of the regulatory and policy landscape, should give particular consideration to the following principles:

- *acknowledge that tech (and trust) is global* — seek to adopt practices and enhance legal and regulatory frameworks in ways that are consistent with international best practice — so that local technology companies are well positioned for international expansion and

[1] These Principles are also available for download at https://www.atlassian.com/blog/technology/regulating-technology.

operation, and Australian consumers and businesses continue to get the benefits, including the security benefits, of global technology suppliers;

- *engage with the issue* — because effectively managing cyber security risks involves a complex set of actors with different roles and responsibilities, policy responses should seek to manage for this diversity rather than relying upon "one size fits all" requirements that may impose unwarranted greater burdens on some sections of the ecosystem or supply chain;
- *define the playing field* and *treat the ailment, don't kill the patient* — consider and assess new regulatory and policy proposals for cyber security in a holistic and consistent manner, having regard to whether and how they respond to and seek to address the specific issues and problems involved; and
- *build the foundation for shared success* — seek to understand and take into account how organisations operate, manage cyber security and respond to incidents and target reforms to ensure that they will be effective within that context.

We believe that these principles, when applied to the issues canvassed in the Discussion Paper, demonstrate a need for clear, actionable and internationally-aligned standards, expectations and guidance.

Having regard to the overarching principles outlined above and given the broad nature of the Discussion Paper, our more specific comments on several of the key themes outlined in the Discussion Paper are set out below.

Enhancing and harmonising regulatory frameworks

Atlassian strongly believes that well-considered and designed laws can help to foster trusted environments in which both businesses and consumers can grow and thrive. In this vein, we appreciate that new and enhanced legislative and regulatory mechanisms can send a signal to organisations and individuals that cyber security is taken seriously, and therefore help to drive the right organisational behaviours when it comes to cyber security risk management.

However, any new frameworks would necessarily be situated within an already complex regulatory environment. According to the 2021 Department of Home Affairs Discussion Paper on *Strengthening Australia's cyber security regulations and incentives*, there are (or were at that time) "at least 51 Commonwealth, state and territory laws that create or could create, some form of cyber security obligation for businesses".[2] Further, these are not the only requirements that Australian organisations must grapple with: many organisations would be required to integrate applicable domestic compliance requirements with their own requirements, industry best practice recommendations and global compliance obligations that apply in the jurisdictions where they — or any of their customers — are located.

Most importantly, protecting Australians from the growing cyber security threat landscape requires a "whole of economy" approach that is capable of reckoning with this complexity. There is no simple solution to protecting Australian consumers from cyber risks, nor is there an individual or group of actors who can singlehandedly reduce the threat of cyber harm.

This is why, before moving to develop new legislative or regulatory mechanisms, we encourage the Government and the Expert Advisory Board to conduct a comprehensive review of these existing laws and frameworks, with the following objectives:

- ensuring that existing legislative frameworks will help to meet the Government's objective of making Australia the most cyber secure nation by 2030;

[2] Viewed at: https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf

- assessing whether any elements of these existing laws add unnecessary complexity or misaligned incentives;
- considering in-progress or recently passed reforms that are not yet fully implemented (such as reforms to the Privacy Act and recently made instruments under the amended Security of Critical Infrastructure Act (**SOCI**)), and the extent to which further clarification, guidance or review of those reforms is required to maintain alignment of incentives; and
- identifying where any gaps in the existing frameworks arise, and whether these might be best addressed through law, regulation or other measures and instruments (including standards and guidance).

In the development of future regulatory arrangements and reforms, we encourage a principles-based approach that aligns to these objectives and does not presume a specific legislative outcome. In addition, and aligned with Atlassian's policy principle *acknowledge that tech (and trust) is global*, we encourage the Government to continue to leverage existing standards and international best practice where possible, rather than creating new localised requirements.

One illustration of this approach can be seen in the recent co-design process for the Risk Management Program Rules under SOCI, which were only made in February 2023 and are still in the process of being implemented. The cyber security aspects of those rules are in certain key respects aligned with existing local or international standards already in use in Australia to assess good cyber security practice. This experience also leads to two further conclusions:

- While we would caution against further significant amendments in the critical infrastructure security arrangements, clarifying how the existing cyber security requirements apply to a critical infrastructure operator's supply chain (including through guidance) would present an opportunity to better protect critical infrastructure and drive better cyber security practice into smaller companies who provide goods and services to those operators.
- More broadly, and as further expanded upon below, Australia should seek to be more active in international standards setting fora, to ensure that Australian needs are being met in the development of international cyber security standards.

Strengthening Australia's international strategy on cyber security

As noted above, Atlassian strongly believes that the best cyber security outcomes will be achieved through consistent, achievable and interoperable standards.

In this respect, it is important to note that many efforts are underway globally to develop and clarify regulatory expectations and corresponding standards with respect to cyber security. This includes efforts by Australia's key allies and trading partners, and extends to the definition of standards that will influence how technology products and services are designed and offered in those markets.

For example, both the US and EU are actively considering standards related to secure software development, and the processes and practices that should accompany those standards, including the format for the production of Software Bill of Materials (SBOMs). These parallel processes would significantly benefit from the development of unified international standards to avoid adding cost and complexity to globally-focused software development processes and ultimately increasing confusion for software users already dealing with a growing number of local and international security standards.

As an important economic and strategic partner to both the US and EU, we believe that there is a significant opportunity for Australia (alongside other likeminded jurisdictions) to seek to leverage the Strategy to actively engage with its counterparts to explore the development of those unified standards.[3]

Supporting Australia's cyber security workforce and skills pipeline

We believe that the number one factor that would both grow Australia's cyber security industry and develop Australia's workforce is access to skills and training, with an eye towards broad technical skills to ensure that technology is developed and deployed securely (rather than being limited to cyber security-specific skills focused on protecting systems and responding to incidents).

The ACSC's 2020 report on Cyber Security and Australian Small Businesses[4] identified a lack of dedicated IT staff as one of the largest barriers to implementing good cyber security practices within an organisation. It also found that, in many smaller organisations, responsibility for security often resides with a staff member with a broad range of responsibilities. The smaller the business, the less likely it is that the business even has a dedicated IT professional, let alone someone dedicated to cyber security, on staff.

The availability of IT skills across the economy should remain a critical focus for the Government broadly, but specifically in the context of cyber security. This is why Atlassian is a strong supporter of the Tech Council of Australia's goal — adopted by the Government and cited in the Discussion Paper — to employ 1.2 million people in tech jobs by 2030.

To hit this target requires a whole-of-system approach to skills development, including entry-level training and education, retraining/reskilling and skilled migration.

A lot of technology training already occurs outside of the nationally-accredited Vocational Education and Training (**VET**) system, leveraging industry-developed training. If we want Australians' skills to maintain pace with the fast-moving technology — and consequently the cyber threat — landscape, then we need to remove barriers to integrating fast-moving industry content into the nationally accredited training system.

The current process for integrating industry content into nationally accredited qualifications requires a complex mapping of industry training material and curriculum with Units of Competency. This causes a lack of incentives in the system for young students to do industry-relevant training and for businesses to develop entry-level pathways. There are also challenges in recognising existing skills (to enable faster training of candidates) because of the cumbersome recognition of prior learning process in the VET system.

Moving to an industry-aligned skills standards based on objective testing criteria — aligned to existing international frameworks like NIST's National Initiative for Cyber security Education (**NICE**) or the broader Skills Framework for the Information Age (**SFIA**) — that is less explicit about the method or time of training allows for a person's existing skills to be tested to help fast-track training.

A standards-based approach also broadens the pool of possible training providers, with the governance around funding shifting towards the outcome of the training as opposed to governing the mechanism of training. If the skills standard is agnostic of training method, it can then also be used to assess learners through other pathways including micro-credentials or full degrees through universities or non-traditional bootcamp-style training.

There's also an opportunity for us to work with international partners, such as the US and UK, on cross-recognition of a certified skills standard and testing framework.

[3] Atlassian acknowledges the significant progress on this front through Australia's lead role in the recently announced multilaterally-supported security-by-design and -default guidance – which we explore further in a later section of this submission.

[4] Available at https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf.

Designing and sustaining security in new technologies

As we mentioned at the outset, responsibility for cyber security is shared by all of us. We believe that this shared responsibility is and should remain at the core of the Strategy, and is embedded throughout the “whole of economy” and “whole of system” focus of this submission.

We believe it is important to note that this conception of a shared responsibility model is and has held true when it comes to allocating responsibility for the adoption and use of technology more broadly throughout time, regardless of which technology is at issue.

While roles and responsibilities of producers and users of technology may differ depending on the type of technology and the deployment model, both will always have a part to play in maintaining the security of systems and data related to those technologies.

At Atlassian, we make collaboration software which is made available in one of two broad types of deployment models: downloaded and installed on customer-managed infrastructure (**on-premise**) versus Software-as-a-Service (**SaaS**) models deployed on cloud infrastructure managed by the service provider. The roles and responsibilities of Atlassian as a software provider, and its customers and users, differ greatly depending on the deployment model chosen:

- In the on-premise scenario, while the software developer is ultimately responsible for ensuring that the software is developed as securely as it can be, and that potential vulnerabilities are identified and managed, it is the end users who are responsible for ensuring that the software is upgraded and that security patches from the developer are deployed. The end user is also responsible for physical, infrastructure, network security and integrations to other systems related to that application.
- In a SaaS deployment, the service provider manages updates, patching and all of the physical, infrastructure and network security related to that application, with all end users gaining the benefit of those security processes. In this scenario, the end user may still be responsible for security relating to access to that application such as passwords, identity management and authentication; any security related to the integration and operation of that SaaS application with other applications; and the management and security of devices that are used to access these applications.

As noted above, this allocation of responsibilities may also involve a variety of additional providers and elements of the user’s technology environment with which the relevant software may interface and interact. This allocation of responsibilities across the supply chain and technology environment should be kept in mind when formulating new or enhanced regulatory arrangements, as measures that have the effect of disrupting this allocation could have the unintended consequences of failing to incentivise good security practices from *both* producers and end users.

To this end, we note that the cyber agencies of seven nations, including Australia’s ASD and ACSC, released jointly-sponsored guidance on 13 April: *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default* (the **Guidance***)*.[5] The Guidance urges software developers to adopt a range of secure-by-design approaches and implement secure-by-default controls within the out of the box configuration of the software.

We welcome this coordinated and significant multilateral effort to improve the security of software. Given it is likely that the Government and the Expert Advisory Board will consider the Guidance within the scope of its review, we wanted to provide our perspective on it.

On the first section related to secure-by-design, Atlassian supports the promotion of secure software development practices, frameworks and standards along the lines of those within

[5] Viewed at: https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default

the Guidance, including NIST's Secure Software Development Framework (**SSDF**). We note that the majority of the secure software development standards, including SSDF, cited in the report are relatively nascent and have not yet achieved global acceptance, nor do they have the necessary supporting infrastructure required to adopt, implement, and verify such requirements at scale. We support efforts to build out this necessary infrastructure across the public and private sectors.

We believe that this can and should be achieved by:

- Implementing a standards-based approach, whereby software developers can attest (and as standards processes mature over coming years, potentially produce independent verification or audits) that their practices align with these standards, and can give customers assurances that the software they are purchasing has been developed in a secure way. Based on experience with similar standards that assess broader security arrangements, procurement, and contractual mechanisms — including responsibilities on the technology producer to continue to ensure that the products remain secure during their supported or contracted lifecycle — are also likely to be the most appropriate and efficient way to implement such controls and incentivise these practices.
- Australia continuing to work with strategic international partners – including the joint signatories to the Guidance – to support international standards development and/or the global implementation of emerging frameworks such as SSDF, so that Australian software producers can implement development processes in ways that can be assessed globally.

On the Guidance's second section related to secure-by-default, Atlassian urges that implementation of such requirements that override potentially valid customer choices require further, careful consideration and clarification.

For example:

- The ability for software providers to control the implementation of software can vary by deployment model. Some default controls that software providers can implement under a SaaS deployment may not be appropriate in an on-premise deployment, where the customer ultimately controls the environment in which the software operates and is likely to want greater control over its configuration.
- Some of the tactics under secure-by-default – including *Forward looking security over backwards compatibility* – are already the preference for most software providers but can be difficult to implement due to strong customer demands. Therefore, such tactics need to be supported by efforts within key customers, such as reducing the use of legacy software, particularly within government agencies.

Any additional requirements on software developers should ultimately be considered as part of a comprehensive balancing exercise to avoid creating the wrong incentive structures, confusion over roles and responsibilities, and potentially entrenching existing poor security practices.

Improving public-private mechanisms for cyber threat sharing and blocking

We appreciate the Discussion Paper's acknowledgement of the opportunity presented by the Strategy to improve information sharing arrangements between the private and public sector.

The biggest step forward to improving the sharing of cyber information would be to remove the costly, time-consuming, and personally burdensome requirement for a security clearance to receive classified intelligence. This requirement adds a disincentive to businesses and their employees engaging effectively with the Government (outside of those who work and transact with secure government agencies on a day-to-day basis and require such clearances as part of their ordinary business operations).

Most Australian businesses do not have those day-to-day transactional requirements for security clearances but are already comfortable with legally-enforceable non-disclosure agreements or deeds that enable the sharing of sensitive information with commercial partners (including cyber security information and highly valuable trade secrets). While the Australian Government does use such arrangements at its discretion, it is not encouraged.

Removing these strict requirements for security clearances – while maintaining the strong legal sanctions for the disclosure of such information through other mechanisms – would increase the number of Australian businesses able to engage with the Government on security matters, particularly for infrequent intelligence briefings or threat information sharing. If these engagements can include actionable, classified intelligence, it will improve the value of these engagements for business, increase the chances of their active participation in them and likely garner a greater willingness to provide actionable cyber security intelligence in return.

Atlassian would be pleased to discuss these comments with the Department and the Expert Advisory Board, and looks forward to and supports the ongoing development of the Strategy.

Yours sincerely,

David Masters
Head of Global Policy & Regulatory Affairs
Atlassian

Anna Jaffe
Director of Regulatory Affairs & Ethics
Atlassian