We welcome the opportunity to respond to the Department of Home Affairs consultation to increase data security. The initiative is a unique opportunity to establish the clear foundations that will enable greater use of data that is inherently at the core of digital transformation.

In 2023, Microsoft will celebrate being part of Australia's tech ecosystem for 40 years. With over 2,000 employees based in every state and territory in Australia, and over 9,000 partners who are predominantly small businesses employing 200,000 Australians, we have a deep history of investing locally, including in data centres that power Governments, businesses, schools and universities, and the not-for-profit sector in Australia.

We believe that having a coordinated set of clear principles in data security that promote proven virtual controls, such as encryption, and demand international best practice from its agencies and service providers is the best method to increase security while ensuring effective service delivery, a reduction in cost and the stimulation of additional growth in the economy.

The Current Regulatory Environment

Coordination and alignment ***should be focussed on reducing unintended regulatory burden and delays to project timelines by using a develop once use many philosophy to key data issues, especially core definitions and international standards.*** By adopting a common underlying definitional framework, the Government will be able to engage on specific bespoke issues to individual programs and avoid re-litigation of established norms. As the department that is tasked with coordinating and developing national security policy across the Australian Government, home affairs is a natural home to drive this coordination.

As you will be aware the Australian Government has recently developed and consulted on a wide range of interlinked policy initiatives to your own; including, the Australian Data Strategy; the Department of Home Affairs' critical infrastructure legislation consultation process; the Department of Home Affairs' consultation on cyber regulation for the economy; the Digital Transformation Agency's Data Hosting Certification Framework and the wide-ranging review into electronic surveillance reform. These initiatives have different outcomes and scope of responsibilities but in some way are all addressing similar core issues around defining government data; defining data security; defining an appropriate suite of core standards; and defining 'data at rest' and 'data in motion'. ***Providing a clear framework to address and then align foundational data issues, such as definitions, is one of the most important initiatives that this overarching policy can provide.*** A repeatable model will allow the Australian Government to have an efficient ongoing process to address issues as they arise with emerging technologies and techniques.

We firmly believe that across these several different initiatives traditional security controls in personnel security and physical security have been comprehensively covered. We would encourage the Department of Home Affairs to address the remaining control, virtual controls for data that has not been covered by previous regulations and as we have seen in Ukraine are the most important in times of conflict. We would also encourage the department to undertake a coordinated education campaign on the legal framework that underpins international warrants and data exchange. With so many regulations and agreements having been introduced in a relatively short time we think there is considerable benefit in upskilling data security, ICT and cyber security specialists within the Commonwealth and the states and territories.

For example, we engage closely with our government partners on data security and many areas of government are unaware of key information, such as the below taken from the Department of

Home Affairs website, on the Australia-US CLOUD ACT Agreement: *The Australia-US CLOUD Act Agreement enables US agencies to send orders through the US designated authority to Australian communications providers for the purpose of preventing, detecting, investigating or prosecuting serious crime. The IPO framework in the TIA Act lifts the barriers that would otherwise prevent Australian communications providers from responding to such orders;* and *The US will be prohibited from targeting Australian persons under the Agreement, including citizens, permanent residents, corporations, non-incorporated associations like charities, government entities and persons physically located in Australia. Likewise, Australia will be prohibited from targeting US persons.*

The Current International Environment

The importance of proven cyber defences to protect key datasets has been clearly demonstrated in Russian invasion of Ukraine. The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls, and oceans. And the internet itself, unlike land, sea, and the air, is a human creation that relies on a combination of public and private- sector ownership, operation, and protection.

Microsoft security teams have worked closely with Ukrainian government officials and cybersecurity staff at government organisations and private enterprises to identify and remediate threat activity against Ukrainian networks. In January of this year, when the Microsoft Threat Intelligence Center (MSTIC) discovered wiper malware in more than a dozen networks in Ukraine, we alerted the Ukrainian government and published our findings. Following that incident, we established a secure line of communication with key cyber officials in Ukraine to be sure that we could act rapidly with trusted partners to help Ukrainian government agencies, enterprises and organistions defend against attacks. This has included 24/7 sharing of threat intelligence and deployment of technical countermeasures to defeat the observed malware.

We believe there are a number of conclusions from the Russian invasion of Ukraine that are critical when considering data security in Australia.

- First, defence against a military invasion now requires *for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries*. Russia not surprisingly targeted Ukraine's governmental data center in an early cruise missile attack, and other on premises servers similarly were vulnerable to attacks by conventional weapons. Russia also targeted its destructive "wiper" attacks at on-premises computer networks. *But Ukraine's government has successfully sustained its civil and military operations by acting quickly to disburse its digital infrastructure into the public cloud, where it has been hosted in data centers across Europe*. This has involved urgent and extraordinary steps from across the tech sector, including by Microsoft. While the tech sector's work has been vital, it's also important to think about the longer-lasting lessons that come from these efforts.
- Second, recent *advances in cyber threat intelligence and end-point protection* have helped Ukraine withstand a high percentage of destructive Russian cyberattacks.
- Finally, the lessons from Ukraine call for *a coordinated and comprehensive strategy to strengthen defenses against the full range of cyber destructive, espionage, and influence operations*

Today, governments rely on digital communications and data, and one key to sustaining the Ukrainian government has been to disburse these digital operations into the public cloud and outside the country itself.

Prior to the war, Ukraine had a longstanding Data Protection Law prohibiting government authorities from processing and storing data in the public cloud. This meant that the country's public-sector digital infrastructure was run locally on servers physically located within the country's borders. A week before the Russian invasion, the Ukrainian government was running entirely on servers located within government buildings—locations that were vulnerable to missile attacks and artillery bombardment.

Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, and his colleagues in Parliament recognized the need to address this vulnerability. On February 17, just days before Russian troops invaded, Ukraine's Parliament took action to amend its data protection law to allow government data to move off existing on-premises servers and into the public cloud. This in effect enabled it to "evacuate" critical government data outside the country and into data centers across Europe.

We would encourage the Government to engage with our sector, through a detailed workshop process, on the lessons learnt in cyber security and data security from the Russian invasion of Ukraine.

We also encourage the Department of Home Affairs to consider closely the actions surrounding the Ukrainian Data Protection Law and subsequent amendments.

Meaningful Options to Increase Data Security

Given the interconnected nature of IT systems and a threat aperture which is global, threats can come from and target any location. Our view is that the locality of your data in the Microsoft cloud is not considered a security control for data, but is an architectural choice when building applications. In essence, with the correct security controls in place, on the Microsoft Global Network of data centre regions, your data is no more secure in the Sydney data centre than it is in Washington, Auckland or Paris Microsoft data centres.

This is an area that is largely still misunderstood in the market, and misconceptions regarding threats such as Insider Threat or Law Enforcement Access Requests still exist. If this is an area of concern, we would welcome the opportunity to brief policy makers on these matters.

When it comes to data security, in a hyper-scale cloud context, it is important to note that scale, capability, investment and maturity are fundamentally important factors in improving data security. Microsoft analyses over 24 trillion security signals every 24 hours offering a uniquely comprehensive view of the current state of security and we have more than 8,500 Microsoft security experts from across 77 countries that help to provide a critical perspective on the security landscape.

Organistions that effectively manage the lifecycle and flow of their sensitive data as part of their business operations make it that much easier for data security and compliance teams to reduce exposure and manage risk.

Securing devices to secure data

Through extensive research and testing, Microsoft identified the seven properties that are present in all standalone, internet-connected devices considered to be highly secured. In many cases, these highly secured devices apply additional security measures, but in all cases each of the seven

properties is present. Collectively, these seven properties provide a baseline foundation of security throughout device silicon, software architecture and OS, cloud communications, and cloud services. The complexity of maintaining all seven properties could be a barrier for some organistions, despite the exceptional cost that often results from a fallout of incomplete device security.

1. Hardware root of trust
2. Defence in depth
3. Small, trusted computing base
4. Dynamic compartments
5. Password-less authentication
6. Error reporting
7. Renewable security

We strongly encourage the Department of Home Affairs to consider a baseline foundation of security approach.

The Value of Encryption

To protect the confidentiality of customer content, Microsoft online services encrypt all data at rest and in transit with some of the strongest and most secure encryption protocols available. Encryption complements access control by protecting the confidentiality of customer content wherever it's stored and by preventing content from being read while in transit between Microsoft online services systems or between Microsoft online services and the customer. ***We would encourage the Department of Home Affairs to clearly state the importance of strong encryption when securing data to encourage greater take-up of modern encryption and practices by governments and critical infrastructure.***

Encryption is a key component to protecting files and organistional information, but it's important to understand the details of how encryption works. Encryption by itself doesn't prevent content interception. Organistions need to have a larger data protection strategy to ensure only authorized parties can use the encrypted data. Encryption can, and more importantly should, co-exist in multiple layers operating at the same time - such as encrypting both the email message and the channel it flows through. Different layers of encryption can help achieve different business goals, such as safeguarding sensitive content or helping meet regulatory obligations. A robust business strategy uses multiple layers of encryption together enabling the business to meet both internal and external data protection requirements. ***We recommend that Australian Government organisations should develop and put in place a content encryption strategy to safeguard content.***

Data Security & Privacy

We feel government should be clear on the benefits of privacy enhancing technologies, and how control stays with the data owner and protects them against malicious harm, as well as puts them in control should a government request access to data for law enforcement purposes. Privacy enhancing technologies are available today to ensure appropriate security of data, as well as the controlled use of the data.

We feel strongly that the data security debate in Australia is fundamentally important in realising the Government's ambition to be a world leading digital economy. The scale of international threats is increasing to the point where ransomware and other international cyber threats are fundamental considerations when developing data policy. There is no way for Australia to insulate or isolate itself

from international cyber threats. Australia must have a mature outlook and ensure that the government and economy has access to the most advanced research and engineering.

Using advanced encryption technology; having access to rapid threat intelligence; and the ability to leverage world-leading engineering capacity are among the most important factors in securing Australia's data. Data security policy should be focussed on transitioning Australia's debate from one based on historical issues such as data locality to the key requirements of a modern digital environment, a focus on capability, capacity and controls.

At Microsoft, we recognize that our customers entrust us with their most valuable asset—their data. As such, we focus on allowing customers to make meaningful choices about the data they share, and we are committed to transparent communication about how we use that data across our products and services.