By online submission
Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

RESPONSES TO QUESTIONS ON NOTICE FROM
08 JULY 2021 PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
(SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020) HEARING

1. **What is your understanding of the software the Bill enables the Government to install on your networks through the Government Assistance powers?**

As a hyperscale cloud provider, Microsoft operates a complex, interdependent system of networks. These networks function in an airtight ecosystem maintained at high cost and with a rigorous level of attention. Although the Government has not specified the type of software that it would seek to install, the installation of *any* software or equipment will almost certainly cause significant collateral consequences on our networks. Specifically, the installation of such software threatens to:

1. introduce vulnerabilities into our networks;

2. compromise interdependent systems relied upon by customers, many of whom are organisations responsible for critical infrastructure assets; and

3. introduce a serious risk of interoperability problems stemming from the requirement for the Government's tools and software to be able to be deployed safely and reliably in various environments with very different system and security architectures.

These risks are especially likely in hyperscale cloud environments, which are built using technology that differs to that in standard cloud deployments and data centres. Any third-party tools introduced into that environment are therefore unlikely to operate or produce the results expected, and are likely to create foreseeable collateral consequences.

Consequently, rather than creating a more secure ecosystem, the prospect of the Government installing software on our systems and networks creates substantial third-party risk to Microsoft and our customers. As noted in our submission and testimony, Microsoft operates horizontally across industries and sectors, and the installation of third-party software will undermine the security of not just our own networks, but the operations of our various critical infrastructure customers who rely on our networks. We therefore believe that the installation of any software would undermine the overarching goal shared by Microsoft and the Government—namely, to preserve the confidentiality, integrity, and availability of critical infrastructure.

2. What is the threshold for which you would accept this intervention?

As referenced in our testimony, Microsoft appreciates that the Government is asking the Committee to legislate for a worst-case scenario in which a critical infrastructure operator refuses to cooperate with the Government during a cybersecurity incident. However, we strongly emphasise that it is also the responsibility of the Committee to guard against a second worst-case scenario: unintended future Government overreach into the operations of a hyperscale cloud provider.

We appreciate that the Government stands ready to assist critical infrastructure operators. However, we note that Microsoft is differently situated: we are a sophisticated hyperscale cloud service provider that understands very well how to defend our systems and networks. We have unique, specialised expertise about our own systems and architecture. We also make considerable efforts to better understand attack vectors and threats by investing billions of dollars every year in threat analysis and security improvements. We therefore cannot envisage an attack scenario in which Government intervention would improve our response, and in the interests of security of Australian critical infrastructure organisations, we would not be receptive to such intervention. That said, we have a long history of standing in partnership with the Government, and have specifically relied on the Government to share its expertise with organisations that may not have the resources or ability to improve their cybersecurity.

3. Have you ever sought Government Assistance?

Microsoft has not sought Government Assistance as defined in the draft legislation. However, we have worked extensively with the Government and pride ourselves in our collaborative and cooperative relationships with agencies and organisations across the Government.

By way of example, during the recent Microsoft Exchange attacks, we were made aware of a vulnerability affecting our boxed Microsoft Exchange product—which we note is *not* the version of Exchange that runs on the cloud, but rather software that assists operations on-premises[1]. Microsoft worked immediately to remediate the issue, using our expertise, agile engineering capacity, and threat analytics tools. We introduced a security patch, worked with government partners in the United States and Australia to raise awareness of the issue, and reached out to organisations. Additionally, we engaged with the Australian Cyber Security Centre (ACSC) very early in the process and maintained a working relationship with ACSC to reach the broadest sphere of Australian organisations that may have been impacted by the vulnerability.

4. When or in what circumstances would you call the Government in to install software on your network?

Microsoft values our engagements and partnership with the Australian Government. However, Microsoft is best positioned to defend our networks, having invested billions of dollars annually to perform threat analyses and design and implement security improvements. Due to the size and complexity of our networks and systems, the installation of *any* software or equipment will almost certainly cause significant collateral consequences, as detailed in our response to the first question above. We therefore would not call on the Government to install software on our network – in fact, to do so may not only breach our

[1] Note: Microsoft cannot monitor a customer's on-premises network; however, were this to have occurred in the cloud, we could have helped identify anomalies and protected our customers.

contractual and legal obligations to our customers, but also would introduce considerable risk into our environment and threaten the security of our broader customer base.

5. **Confirm that the evidence provided from the Director-General of the Australian Signals Directorate (at page 28 of the Hansard transcript for the Committee's 11 June hearing) could not refer to your company.**

We confirm that the evidence provided by Director-General Noble could not refer to Microsoft.