Quad Cybersecurity Partnership: Joint Principles

1. To deliver Quad Leaders' vision for a free, open and resilient Indo-Pacific, the Quad Senior Cyber Group confirms the following principles aiming to guide cyber security cooperation between partners and support cyber security uplift across the Indo-Pacific region under our Quad Cybersecurity Partnership. Quad members recognize the need for improving cybersecurity in an increasingly digital world with sophisticated cyber threats. As partners, we seek to cooperate to enhance the development of: critical infrastructure cybersecurity, supply chain risk management, software security, workforce development.

2. The critical infrastructure that our citizens rely on for every day essential services is increasingly at risk from cyber threats. The interconnected and interdependent nature of critical infrastructure, without proper cyber security safeguards increases that risk and can deliberately or inadvertently cause disruption and subsequent economic and security concerns within and across borders. The consequences of a prolonged and widespread failure in the energy sector, for example, could be catastrophic to our economies, security and sovereignty, as well as our way of life.

3. Recognising the key role industry and governments play in the ongoing protection of critical infrastructure, Quad members will work together and with relevant industry and non-government stakeholders for the development and implementation of cyber security and critical infrastructure protection policies. Quad members commit to share approaches to policy development to augment security and share threat information between our governments and with industry partners in a rapid and timely fashion to develop a resilient ecosystem. We will work together to improve the security of the technology products and services on which our critical infrastructure provider rely.

4. We understand that the assets, systems and networks of our critical infrastructure sectors are so vital that their incapacitation or destruction would have a debilitating impact on national security, economy, public health and safety. Secure and resilient Information Technology (IT) and Operational Technology (OT), and the supply chains for digitally enabled products and services, help ensure that our businesses and consumers get the products they need to protect their networks and systems. Transparency, information sharing, diversity, openness, predictability and sustainability are essential elements for trusted and resilient supply chains. Governments and industry can work together to identify potential risks and develop frameworks to evaluate supply chain risk dependencies as it relates to cyber security, ensuring this aligns with our work in the Quad Critical and Emerging Technology Working Group. We will continue to exchange views on standards, baselines, guidelines and procedures, through a consultative process by governments and industries followed by periodic review of appropriate controls and assurance mechanisms, to ensure the sharing of best practices.

5. Quad partners are in a unique position to align and ensure the implementation of baseline software security standards domestically and internationally; the collective purchasing power of our respective governments can drive cybersecurity improvement and ensure security as a basic design consideration. Coordinating our implementation of baseline software standards

will have a significant impact on the cybersecurity of our people, critical infrastructure, and essential services.

6. We will continue to align baseline standards, not only for government procurement, but also across managed service providers and technology products and services within the broader software development ecosystem. Depending on each partners' current activities and industrial situation, these standards could include: improving vulnerability management and applying the latest patches, providing a software bill of materials, using multi-factor authentication, regularly backing up data, encrypting data, and rigorously auditing the security management system, as well as mechanisms for skills and competency verification of auditors.

7. Quad nations will engage in domestic efforts to implement the above mentioned standards and commit to jointly align the development of software security frameworks for government software procurement. We believe this approach will enhance government cybersecurity while also driving market change in software security. Engagement with domestic industry stakeholders is also an essential element of this effort, because the private sector will ultimately implement these requirements and work with Quad governments to continuously adapt them to the growing threat environment. We seek an open and collaborative relationship with industry to implement minimum software security standards for government procured software. These engagements can and should lead to broader conversations outside procurement channels about how best to adopt these minimum standards across the software development ecosystem.

8. We share serious concerns over ever more complex and destructive threats stemming from malicious cyber actors and the risks they pose to national security, and affirm our commitment to enhance the coordination of respective efforts to strengthen capacity building of the Quad members and their partners across the Indo-Pacific region. Quad countries will collaborate on capacity building programs in the Indo-Pacific region to further enhance their efforts, through the Quad Cybersecurity Partnership.

9. We reaffirm the importance of enhancing collective efforts to increase our cybersecurity workforce, based on the shared recognition that cyberattacks are increasing and becoming more complex, and we also share the challenge of generating adequate expertise. In addition to capacity building, Quad members will work together to enhance our collective cyber security workforce and pool of talented cyber professionals.

10. These principles will drive cooperation of the Quad Senior Cyber Group to address common challenges and allow us to seize the opportunity to improve cyber resilience in a rapidly-changing threat environment. We have come together with a shared purpose and committed to goals that are ambitious, pragmatic and action-oriented.