STATEMENT BY THE REPRESENTATIVE OF AUSTRALIA TO THE INTER-SESSIONAL MEETING OF THE OPEN ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS (DECEMBER 2022)

Confidence Building Measures (CBMs)

Australia is pleased to deliver this intervention in our national capacity, as part of a joint and sequenced approach by a cross-regional group of state confidence builders

- and Australia thanks Israel, Chile, Singapore, Canada and Germany for their considered interventions, and looks forward to the contributions of Mexico and the Netherlands, to follow.

Australia would like to take this opportunity to briefly discuss those confidence building measures focused upon transparency.

While transparency measures were originally developed in an entirely different context – namely to build confidence with regard to the proliferation and use of conventional weapons – the traditional approach to military and non-military CBMs has required certain adaptations in order to adequately reflect the specificity of cyberspace.

The importance of transparency measures to peace and security in cyberspace has been recognised and emphasised by this group and its predecessors since 2013 – we all know that transparency breeds accountability and stability.

But we recognise that transparency can raise sensitivities. As with many other aspects of our framework of responsible state behaviour, transparency measures should always be voluntary, the type and detail of information to be determined by the participating state.

While transparency measures strive to eliminate the elements of secrecy that can lead to misperceptions, transparency measures must also enhance, rather than endanger, the participating states' national security: transparency doesn't mean no classification.

If participating states are secure in the knowledge that transparency CBMs do not undermine, and, in fact, may be beneficial, to their own national security, the measures have a greater chance of being sustained and developing into further cooperative activity.

The assumption is that exchange of information and resources contributes to stability by enhancing situational awareness and building common understandings.

The types of information that may be appropriate to share, and the forum in which to share it, can be discussed, promoted, and recommended by this group, but should always ultimately be at the discretion of the participating states.

Some examples of transparency measures that the Open Ended Working Group (OEWG) could promote and provide best practice for include:

- As recommended by the 2021 OEWG and 2022 annual progress report: sharing relevant information on policies, strategies, regulatory and legal frameworks – particularly through the United Nations Institute for Disarmament Research (UNIDIR) cyber policy portal – and ensuring states' contributions to the portal remain up to date
    - For example, Australia's entry on UNIDIR's portal includes links to our international cyber engagement strategy, which sets out Australia's policy priorities for international security in cyberspace
- As recommended by the 2015 Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE): sharing national views and information on aspects of cyber threats (both national and transnational) and national policies to address those threats
    - For example, the Australian Cyber Security Centre regularly publishes threat reports, and Australia's cyber security strategy (also available on the UNIDIR portal) sets out Australia's policy and regulatory framework to address those threats

- The 2021 GGE report provided additional detail on the types of information that, when countries increase transparency, could increase trust and stability, including: national approaches to ICT and cyber security, data protection, protection of critical infrastructure, and the missions, functions, organisational structure, legal and oversight regimes of states' ICT security agencies.

Additional transparency measures which we invite further discussion on in the OEWG include:

- publishing documents and doctrine and sharing approaches to addressing threats or harmful ICT practices
    - because even where no direct cooperation takes place, this transparency can also help build trust and confidence between States
- Initiating bilateral/trilateral/plurilateral cyber policy dialogues that foster discussion on issues of international peace and security in cyberspace
- Developing transparent procedures to respond to appropriate notifications of Cyber incidents from other governments
- Publishing and sharing government policy on issues pertaining to international peace and security in cyberspace. Such documents should link international efforts to domestic efforts, and provide for meaningful multi-stakeholder engagement, and finally
- Transparency about the policies and procedures that inform operational and strategic responses to cyber incidents would promote common understandings, increase predictability, foster trust and reduces the risk of miscommunication during times of crisis.

Australia firmly believes that enhancing the scope of information sharing is key for building international trust

- And hope that by discussing best practice for transparency measures in this forum, and providing practical examples of implementation of these

measures, we can collectively advance responsible cyber behaviour, and international stability in cyberspace.

Thank you.