## Cybersecurity Tech Accord on Clusters 6-10

The Cybersecurity Tech Accord welcomes the opportunity to address clusters 6-10 today. We fully support the comments of the International Chamber of Commerce, US Council for International Business, and Microsoft on this group of articles.

Madame Chair, today I will be speaking to Articles 27, Production orders; 29, Real-time collection of traffic data; and 30, Interception of content data.

Article 27 should be amended to include a qualification that it is subject to a reasonable belief the offence committed is set forth in this Convention and where jurisdiction can reasonably be claimed over it.

The text should also make clear that a service provider receiving an order must have some legal nexus with the state ordering the production. Without these changes, conflicts of laws problems will arise.

Let me turn to Articles 29 and 30.

We have consistently emphasized – as have many delegations - that these are particularly broad powers with a high potential for abuse, taken out of the Budapest context where the implementation notes address how and when such powers should be used and the overall expected context of checks and balances in the legal system of the implementing state.

Absent robust additional safeguards, these articles should be deleted. An example will show how serious the problem is.

If a state wants to gain access to a government official's communications, it can allege a crime has been committed in its territory and request interception of communications and real-time traffic data from a state that official is travelling to. It would know that person's movements from traffic data, and gain access to their content data. In this scenario neither the accused nor his employer would ever know about any of this. The service providers would be required to participate no matter what, since the Convention doesn't allow them to object in any situation.

This example clearly would be abuse of the Convention, made possible by the lack of transparency, safeguards, and ability of providers to question requests or refuse them.

Adding the safeguards we have consistently called for would prevent this kind of abuse as transparency would ensure the request became visible to those affected. Ironically, adding these provisions also facilitates data exchange for genuine offences increasing trust in the system as a whole.

**Thank you Madame Chair and distinguished delegates.**

We are at the service of all concerned and can be reached as follows:

**During the AHC Session:** Mr. Nick Ashton-Hart, Head of Delegation, at nashtonhart@apcoworldwide.com and+1 202 779-1072

**All other times please email** eravaioli@apcoworldwide.com