UK response to the Global Cyber Agenda Utilization Guidelines consultation on 23 April 2020

We are grateful to the authors of the International Telecommunications Union (ITU) Global Cyber Agenda (GCA) Utilization Guidelines for providing such a substantial document for consideration.

The consultation session on the on 23 April 2020 prompted interesting discussion, and a wide range of opinions and ideas were presented. In future, we request greater consideration of the requirement for consultation and opportunity for reflection of discussion in submitted comments.

The number of people wishing to speak during the meeting was encouraging, but there was little time to take the floor and respond to some of the proposals that we heard. The UK submitted formal written input to the process and also an informal document providing comments, mostly of an editorial nature before the meeting on the 23rd. Both of those documents remain valid. We offer further thoughts here based on the draft guidelines and the suggestions that we heard as an intervention we would wished to have made.

We look forward to reading the next draft of the guidelines, and the opportunity to provide further feedback in the future. We would welcome further clarity as to the process under which these Guidelines will be agreed.

1. **Target audience for Guidelines**. It was clear from the meeting that we, and several others, remain unclear on the target audience for these guidelines. The next iteration must address this central issue.

2. **Maintaining focus on practical support to developing nations.** These guidelines are a major opportunity to assist in supporting developing nations in harnessing the power of Information and Communication Technologies (ICTs). The ITU's remit supports a great deal of extremely valuable work on cybersecurity of real, practical benefit. The ITU must give high priority to this work, and all ITU members should support it, to truly serve its membership in bridging the digital divide and meeting the Sustainable Development Goals. We consider this should be the focus of these Guidelines. Encompassing non-core activities within the Guidelines will risk the delivery of this most important element.

3. **Protecting the reputation of the Global Cyber Agenda.** The guidelines must encourage greater focus and efficiency in work within the ITU, and in projects run jointly between the ITU and external partners. Bringing non-core ITU activities under the GCA umbrella diminishes its overall reputation and effectiveness.

4. **Avoiding undermining existing UN processes.** The UN General Assembly (UNGA) is the key forum for discussion of international peace and security. It also plays a major role in discussions regarding cybercrime. The UK firmly believes that activity under the GCA must not undermine existing discussions in UNGA groupings - the Group of Governmental Experts, the Open Ended Working Group, and the Intergovernmental Expert Group.

5. **ITU remit and Cybercrime.** During the consultation we heard a wide range of opinions regarding the remit of the ITU, and therefore these guidelines, in relation to cybercrime. ITU Plenipotentiary Resolution 130 *Resolves 3* clearly states that cybercrime is a sovereign matter for nations. Any ITU cybercrime work outside the provisions of Resolution 130 is therefore unjustified. The UK does not support it, or its inclusion in the guidelines.

6. We firmly believe there can be no justification for the ITU to draft international law on cybercrime or to modify the ITU treaties to include cybercrime provisions. The Budapest Convention has already assisted many nations to develop and implement effective cybercrime legislation - a key objective of the GCA. Additionally existing discussions in the UN Third Committee already actively address consideration of a UN-led treaty on cybercrime and should not be duplicated.

7. ITU Plenipotentiary Resolution 130 *Instructs the Director of the Telecommunication Development Bureau* clause 2 refers to facilitating access to the work of other international organisations relating to cybercrime legislation, and supporting national and regional capacity building related to cyberthreats/cybercrime. A great deal of valuable has been performed in the D Sector under this 'Instructs' which we fully support.

8. **ITU remit and national capabilities.** We reiterate our particular concern regarding Guideline 1h as drafted. Declarations and guidance relating to cyber sovereignty and policies around lawful interception are outside the remit of the ITU. These are very sensitive issues prompting diverse, strongly held views. This guideline should be deleted in its entirety.