PROTOCOL CONSULTATION PROCESS

The Working Group on Cybersecurity in Arbitration is pleased to announce the release of the 2020 Cybersecurity Protocol for International Arbitration during a panel discussion at the first annual New York Arbitration Week to be held at the New York International Arbitration Center on November 21, 2019. The Protocol also will be featured at the ICCA 2020 Congress to be held in Edinburgh, Scotland in May of 2020, and is available here.

Recognizing that international arbitration in the digital landscape requires reasonable information security measures to protect the information exchanged during the process, the International Council for Commercial Arbitration ("ICCA"), the New York City Bar Association ("NYC Bar") and the International Institute for Conflict Prevention and Resolution ("CPR") established the Working Group to consider appropriate cybersecurity guidance for users of arbitration, counsel, arbitrators and arbitral institutions.

The Working Group published an initial Consultation Draft Protocol that was released at the ICCA Congress in Sydney, Australia in April 2018. The Working Group at that time issued a call for comments that was sent to more than 240 individual consultees representing arbitral institutions, law firm arbitration practice groups, expert witnesses in arbitration proceedings and non-governmental organizations such as bar associations. Since then, the Working Group also solicited feedback at more than 25 public workshops and other events held around the world. The 2020 Edition reflects that feedback and is the current edition of the Protocol. As the subject area is rapidly evolving, the Working Group will solicit feedback from users of the Protocol and anticipates issuing updated editions from time to time in coming years.

Some of the recurring comments that were considered by the Working Group and corresponding changes to the Protocol include:

- Comments that were directly opposed, yet relatively evenly divided, about whether the Protocol should contain more specific advice about technical measures that should be adopted.

  In consideration of these comments, the Working Group has provided additional guidance in Schedule A (previously Schedule C) about baseline security measures that all custodians of arbitration-related information may wish to consider implementing in their individual day-to-day arbitration practices, and has suggested sample procedural language in Schedule D for potential inclusion in arbitration agreements and/or procedural orders.

  At the same time, the Working Group maintains the view that there is no one-size-fits-all approach to information security in arbitration matters and that the risk-based approach adopted by the Protocol, bounded by reasonableness, provides necessary flexibility to accommodate changes in technology, best practices and prevailing cyber risks, as well as the individual circumstances of each case, including considerations such as cost, proportionality, risk tolerance and technical capabilities. Accordingly, the additional guidance that has been added to the Protocol is intended to provide a more useful starting

point for considering what may constitute reasonable cybersecurity measures in the individual circumstances of each case, rather than an endpoint recommendation of any specific, immutable set of technical measures.

- Comments that the Protocol's individualized, risk-based approach leaves security gaps in the arbitral process. Some noted, for example, that consideration of cybersecurity measures at the initial case management stage of an arbitration may be too late, and therefore advocated for institutions to take a leading role in addressing cybersecurity, possibly by establishing a minimum standard of security for matters they administer (such as through the adoption of a secure case platform) and/or by providing (or mandating) arbitrator training.

  The Working Group recognizes and agrees that effective security in an individual matter may require attention prior to the initial case management stage. For this reason, the Working Group anticipates that as general awareness of the importance of cybersecurity to the arbitral process increases, arbitral institutions and others will introduce new initiatives aimed at improving information security in arbitration, some of which may supplement the Protocol. In the interim, the Protocol seeks to fill a significant, existing procedural lacuna in the arbitral process.

- Concern that the Protocol advocates a "top-down," arbitrator-driven approach to determining what cybersecurity measures are reasonable in any given matter.

  The Working Group intended for the Consultation Draft to encourage parties and their counsel to take the lead in determining what cybersecurity measures are reasonable for their individual cases, while also recognizing the important role played by the tribunal. However, as some members of the arbitration community interpreted the Consultation Draft as advocating for a more arbitrator-driven (as opposed to party-driven) approach, the Protocol has been revised to clarify the recommended procedural approach to determining reasonable cybersecurity measures and the relationship between the parties and the tribunal, including that the parties and their counsel are responsible for maintaining the information security measures that they consider appropriate, subject to any directions by the tribunal or the administering institution.

- Comments about what the term "protocol" implies and whether the document is aptly titled as such. According to some commentators, the term "protocol" implies that the document establishes a binding set of cybersecurity rules that must be followed, whereas they perceive the Consultation Draft to be more in the nature of guidelines.

  The Working Group notes that there are multiple meanings of "protocol" and that the term is sometimes used, as the Working Group intended here, to refer to a detailed plan of a specific procedure. Thus, the Protocol establishes a framework that institutions, parties, counsel and arbitrators can consult in order to determine reasonable cybersecurity measures.

  Although the Working Group determined that it would ultimately be more confusing than

not to change the title of the document, in the interest of greater clarity, the revised version of the Protocol is now comprised of "principles" rather than "articles."

Going forward, the Working Group anticipates that there will be ongoing review and revision of the Protocol to take into account practical experience implementing it, as well as changes to technology, prevailing cyber threats, law (including proliferating data privacy regulation across the globe), and emerging consensus as to best practices. Feedback regarding the Protocol may be sent to cybersecurity@arbitration-icca.org.

ICCA-NYC Bar-CPR Working Group on Cybersecurity in International Arbitration
November 2019

Members of the Working Group

Olivier André, International Institute for Conflict Prevention and Resolution (CPR)
Paul Cohen, 4-5 Gray's Inn Square Chambers
Stephanie Cohen, Independent Arbitrator
Hagit Elul, Hughes Hubbard & Reed LLP
Lea Haber Kuck, Skadden, Arps, Slate, Meagher & Flom LLP
Micaela McMurrough, Covington & Burling LLP
Mark Morril, Independent Arbitrator
Kathleen Paisley, International Arbitrator, Ambos Lawyers

Chair: **Brandon Malone**, Scottish Arbitration Centre; Brandon Malone & Company
Secretaries: **Eva Y. Chan** and **Jesse R. Peters**, Skadden, Arps, Slate, Meagher & Flom LLP