**INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)**

FOURTH MEETING OF THE WORKING OAS/Ser.L/X.5

GROUP ON COOPERATION AND CONFIDENCE-BUILDING CICTE/GT/MFCC/doc.3/22

MEASURES IN CYBERSPACE 24 October 2022

October 26-27, 2022 Original: English

Mexico City, Mexico

**CONCEPT PAPER**

Confidence-building measure to facilitate sharing of information about cyber incidents

The Western Hemisphere has seen an increase in notable cyber incidents in recent years. Cyber incidents in our region and around the world have highlighted that incidents may have transnational effects on multiple countries, potentially including effects on critical infrastructure.

This increases the importance of clear communication when a State seeks to convey to other States information about the details or severity of a particular cyber incident. A State may wish, for example, to request foreign assistance with recovery from an incident, share technical information about a threat, or cooperate with other States to respond to an incident.

Cyber incident severity schemas are one mechanism that can facilitate information sharing in such cases. These schemas usually present a ranking system that can be used to categorize a cyber incident based on the severity of its effects. For example, the schema may be color-coded, and a user could describe a cyber incident as being “yellow” or “red” in severity based on the schema. With an established schema in place, a State can refer to it to quickly convey information about a specific incident. As an example, the United States uses the cyber incident severity schema described at [this link](https://www.cisa.gov/uscert/sites/default/files/publications/CISA_National_Cyber_Incident_Scoring_System_S508C.pdf) (also attached).

Our region has already adopted confidence-building measures in cyberspace that encourage information sharing, including on national cybersecurity policies and other documents. By additionally encouraging States to create and share national cyber incident severity schemas in particular, our region could facilitate greater information sharing about cyber threats and cooperation to prevent and mitigate threats. The following new confidence-building measure would address this goal:

* Encourage member states to develop their own national cyber incident severity schemas and share information about them.

States would develop their own schemas. States could share information about their schemas through a mechanism such as the existing online portal that OAS-CICTE administers to facilitate implementation of our region’s confidence-building measures in cyberspace.

Cyber Incident Severity Schema (CISS): [Link](http://scm.oas.org/pdfs/2022/CICTE01561E.pdf)

CICTE01561E01