REGIONAL CONFIDENCE-BUILDING MEASURES (CBMs)
TO PROMOTE COOPERATION AND TRUST IN CYBERSPACE

(Agreed during the First Meeting of the Working Group on
Cooperation and Confidence-Building Measures in Cyberspace,
held on February 28 - March 1, 2018)
REGIONAL CONFIDENCE-BUILDING MEASURES (CBMs)
TO PROMOTE COOPERATION AND TRUST IN CYBERSPACE

(Agreed during the First Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace, held on February 28 - March 1, 2018)

PRIORITY MEASURES

As a result of the initial meeting of the Working Group, experts from the Member States have developed the following initial voluntary cyber Confidence Building Measures (CBMs):

1. Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks, and other documents that each Member State considers relevant.

2. Identify a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. The work of these national points of contact may be distinct from, yet supplement the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern. The information on these national points of contacts will be updated annually, or as frequently as needed, and shared among the national point of contacts in a transparent and readily accessible format.

   Implementation: The Cybersecurity Program within OAS-CICTE Secretariat will maintain and update a repository of documents provided by the Member States, as well as the list of national points of contact identified.

PLAN OF ACTION TO ESTABLISH ADDITIONAL MEASURES

The Member States agree to collaborate at the regional and sub-regional levels to address shared challenges in cyberspace. The Working Group will take the following steps to establish additional CBMs:

1. The Working Group will include in the agenda of its next meeting, the identification and discussion of the cyber threats to the region, including cyber threats to shared critical infrastructure.

2. The Working Group, with input from the private sector and other stakeholders, will develop a prioritized list of key cyber challenges and propose a work plan to address these challenges at the policy level. Results of that discussion will be included in a report to be submitted to CICTE.

3. The Working Group will prepare a list of best practices and lessons learned to guide the response of responsible parties at the policy-making level in the event of a cyber incident involving these threats.

4. The Working Group may review experiences in managing cyber incidents and consider the need for further technical and policy cooperation in this area.
Implementation: The Cybersecurity Program within the OAS-CICTE Secretariat will continue to serve as the Technical Secretariat for the ongoing Working Group. In that role, it could facilitate the suggested meeting and publication of the corresponding report, within available financial and human resources.

PROCEDURAL CONSIDERATIONS

As a result of the initial meeting of the Working Group, Member States acknowledge the benefits of continuing this Working Group as a necessary mechanism, and agree to continue to meet as needed, in person or by digital means, to continue discussion for new and agreed-upon cyber CBMs.

Members of the Working Group agree to recommend that these CBMs to promote cooperation and trust in cyberspace be presented at the Eighteenth Regular Session of CICTE, as a Resolution, and included in the draft Declaration. Likewise, these recommendations should be incorporated in the draft Omnibus Resolution of the Committee on Hemispheric Security to be approved, at the Forty Eighth Regular Session of the General Assembly of the OAS.

Once adopted by the General Assembly, this list of measures will be included in the “Consolidated List of Confidence- And Security-Building Measures” (CP/CSH-1743-16) as a non-traditional measure.