2016 IGF Best Practice Forum on Cybersecurity
Call for contributions
Multi-stakeholder collaboration and cooperation

Prepared by:
The OAS Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States

Disclaimer:
The opinions expressed in this paper do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states.

1. **What are the typical roles and responsibilities of your/each of the stakeholder groups in making the internet a secure and safe place for people to socialize and conduct business?**

   The Program's efforts are geared toward three specific objectives:
   a. Increasing access to knowledge and information on cyber threats and risks;
   b. Enhancing the technical and policy capacity of governments and critical infrastructure operators to detect cyber threats, respond to cyber incidents, and combat both;
   c. Promoting more robust, effective and timely information-sharing, cooperation and coordination among cybersecurity stakeholders at the national, regional and international level.

   The Program's stakeholders include government entities, the private sector, academia, civil society and the general public from the OAS member states. Each stakeholder grouping participates in the cybersecurity supply chain at different stages, either as a supplier or an end-user each has a role to play in keeping their activities secure. As it relates to our activities, each stakeholder grouping has made every effort to participate and contribute to workshops, reports and the develop process for national cybersecurity frameworks. Our workshops include different topics, ranging from critical infrastructure protection to cybersecurity and freedom of speech in the web, and the participation of experts and attendees with different backgrounds. Our reports are prepared based on a comprehensive understanding of cybersecurity with the contributions of stakeholders from different sectors. Our last report, "Cybersecurity: Are we ready in Latin America and the Caribbean?" jointly prepared with the Inter-American Development Bank, is a good example of this collaborative work. Finally, the development of national cybersecurity strategies involves the participation of representatives from different stakeholders since its inception in order to build a common national view on cybersecurity.

2. **What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?**
   a. The OAS Cybersecurity Program has a twitter account which facilitates the easy transmittance of information and communication among the followers.
   b. The OAS Cybersecurity Program has a mailing list in which anyone can participate. This mailing list announces the Program's next activities and recently published reports.
   c. The Program has also been developing a virtual hemispheric network of CSIRTs (csirtamericas.org), which seeks to facilitate real-time communication and information-sharing between CSIRTs in the Americas.
   d. In the development of National Cybersecurity Frameworks, the program facilitates multi-stakeholder roundtables and national workshops to discuss cybersecurity issues facing member states.
   e. The publication of cybersecurity reports that benefits from the input of all member states in providing accurate and current data on their national cybersecurity reality. These re
   f. The hosting of sub regional, regional and international cybersecurity crisis management exercises in collaboration with private sector and national and international government entities.

3. **How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?**
   a. Engagement of political leadership is critical as this will ensure the continuation of cybersecurity initiatives and incorporation of cybersecurity concerns into cross cutting policy issues, such as economic development and national infrastructure expansion projects.
   b. Staging of Regional meetings geared towards networking and building networks on various levels (private sector, academia and government counterparts).
   c. Engagement with stakeholders from different sectors since the beginning of the formulation of cybersecurity policies through participatory and deliberative procedures (e.g., roundtables, online tools) in order to build trust and confidence and ensure the transparency and accountability of the entire process.

4. **What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?**
   a. Exchange of best practices and ideas during regional workshops. These regional workshops provide a unique opportunity for stakeholders from Latin America and the Caribbean to discuss their problems, to share lessons and cybersecurity capacity, as well as to build a common understanding of cybersecurity. The key takeaways of our last regional event are available here.
   b. Assistance for the rectification of cyber incidents through exchange of expertise and information. An example is the assistance of one member state CSIRT going to the aid of another member state who had not yet established national CSIRT capabilities.

5. **What are some examples of best practices in 'Cyber security Situational Awareness' where different organizations have worked together, specifically with law enforcement agencies and other specialists?**
   a. The Program has staged in collaboration with the South School of Internet Governance, 'SEGURINFO' in several of our member states. SEGURINFO is an annual meeting for information security, including an intensive information sessions and networking for information security professionals and industry suppliers.
   b. The OAS is a signatory to and promotes the STOP.THINK.CONNECT messaging Convention. STOP. THINK. CONNECT. is a global online safety awareness campaign aimed at helping people to stay safer and more secure online. The message was created through a coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). Many countries and private sector entities have joined this initiative. (https://www.stopthinkconnect.org/).
   c. In October every year, the OAS Cyber Security Program organizes an event dedicated to raising public awareness about staying secure online in partnership with several organizations, such as the National Cyber Security Alliance, the US Department of Homeland Security, and the STOP.THINK.CONNECT.

6. **What are other related or different topics that your organization would like this BPF to address moving forward, both in 2016 and beyond?**
   a. The intersection of the expansion of broadband connection and the need embedded security.
   b. Development of best practice for contractual arrangements for IT and Information Security services.
   c. Cybersecurity awareness and capacity building for small and medium-sized enterprises (SMEs).
   d. Mechanisms to improve multi-stakeholder collaboration and cooperation in the formulation and implementation of national cybersecurity policies.