OAS Cybersecurity Program

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

OAS Cybersecurity Program
Organization of American States
cybersecurity@oas.org
@OEA_Cyber
Our Mission

**Increased access to knowledge and information on cyber threats and risks** by public, private and civil society stakeholders and Internet users, including vulnerable groups.

**Enhanced technical and policy capacity of governments and CI operators** to detect cyber threats, prevent, respond to, and recover from cyber incidents, and combat cybercrime.

**More robust, effective and timely information-sharing, cooperation and coordination** among CS stakeholders at the national, regional and international level.
What are we doing?
OAS Regional Approach

- CICTE Secretariat
- REMJA Cybercrime (Legislation)
- CITEL (Telecommunications)

- “Inter-American Convention against Terrorism” (2002)
- Declaration “Strengthening Cyber Security in the Americas” (2012)
- Declaration “Protection of Critical Infrastructure from Emerging Threats” (2015)
- Declaration “Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace” (2016)
What the OAS does on Cybersecurity issues?

**Policy Development**
- Development of national and/or regional assessments and strategies

**Institutional Strengthening**
- Establishment/Promotion of National CERTs
- Management of CSIRT Americas
- Tailored technical assistance
- Cyber Exercises

**Research and Outreach**
- Development of technical documents, toolkits and reports
- Creation and management of cybersecurityobservatory.com
- Participation at relevant cyberspace activities
- Communications
National Cyber Security Strategies
Evolving sophistication in cyber attacks that threaten businesses, privacy of personal information and national security must be met by a dynamic and measured response.

Without a strategic response, national cybersecurity efforts will be unsustainable, stove-piped, sporadic, duplicative, and not cost-effective.

Governments’ increasing reliance on ICTs and cyberspace, and accompanying vulnerability and exposure to increased threats and risks of attacks.

Why develop a National Cybersecurity Strategy?
What makes a strategy successful?

1. Commitment at key levels: find a champion
2. Knowing where you are: taking stock and assessing
3. Knowing where you want to be in 5-10 years
4. Identifying and engaging key stakeholders
5. Identifying the steps and milestones to getting there: action planning
6. Ensuring measurable and attainable goals: review and revise
7. Estimating cost attached to activities
Member state appoints a local point of contact, who will be responsible for leading the national cybersecurity strategy development process.

Desk-Study is conducted of country’s existing polices and legislative framework in relation to cyber security.

Questionnaire (developed by OAS) is distributed to key stakeholders identified by the member state to further assess country situation.

Survey results are analyzed and a summary of key findings and emerging national priorities are identified.
In-situ visit is conducted with member state's officials and all relevant stakeholders for the national cybersecurity strategy development process.

Stakeholders are placed in working groups based on broad national priorities and consulted to identify activities, roles, responsibilities, and time frame for implementation and possible costs.

The working group with the support of the OAS prepares a draft taking into account findings of the consultations and international best practice.

Comments and amendments are incorporated.

Draft strategy is validated on another in-situ visit and finalized for adoption and official approval by Government.
National Strategies Adopted

Colombia (2011 & 2016)

Trinidad and Tobago 2013

Panama 2013

Jamaica 2015

Paraguay 2017

Chile 2017
National Strategies under development

- Costa Rica
- Dominica
- Dominican Republic
- Guatemala
- Mexico
- Peru
- Suriname
Thank you!
Merci
Gracias
Obrigado

OAS Cybersecurity Program
Organization of American States
cybersecurity@oas.org
@OEA_Cyber