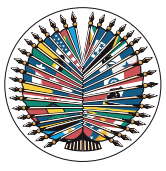
# OAS CYBER SECURITY INITIATIVE

Global Forum on Cyber Expertise (GFCE)



Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

GCCS 2015 The Netherlands

# CONTENTS



## OAS CYBER SECURITY INITIATIVE

The Organization of American States (OAS) has been working to strengthen cyber security capacities in OAS Member States since the early 2000s. Over the years, it has become a regional leader in assisting countries to build technical and policy-level cyber security capacity to ensure a secure and resilient cyberspace. The OAS Cyber Security Program support initiatives based on an in-depth analysis and understanding of the extent of cyber threats in a given country, and of existing national capabilities to deal with such threats. In addition, the OAS promotes the engagement of partners and stakeholders from different sectors, ensuring that government, private sector and civil society directly participate in the formulation of cyber security policies.

## OAS REGIONAL CYBER SECURITY FRAMEWORK

In 2004, the OAS became the first regional body to adopt a Cyber Security strategy through the unanimous approval of "The Comprehensive Inter-American Cyber Security Strategy," which provides a mandate to the OAS General Secretariat to assist Member States in the creation and strengthening of their cyber security capabilities. Recognizing the evolving nature of cyber security threats, OAS Member States renewed their commitment to cyber security by adopting, in 2012, the declaration on "Strengthening Cyber Security in the Americas" (2012) and, more recently, the "Declaration on the Protection of Critical Infrastructure from Emerging Threats" (2015). These instruments are critical for the promotion of politically cohesive cyber security policies in the Americas.

# WHAT WE OFFER TO OUR MEMBER STATES

The OAS Cyber Security Initiative addresses cyber security issues based on a flexible and dynamic approach, in which cyber security policies and the provision of technical trainings are adjusted according to new trends and evolving needs. Over the years, the OAS Cyber Security Program has evolved to address the challenges in a multifaceted and tailored approach, establishing an action plan that can be adapted to best fit a country's specific needs.

## 1. NATIONAL CYBER SECURITY STRATEGY DEVELOPMENT

The OAS Cyber Security Program's approach in this area consists in facilitating the organization of national roundtable discussions with the participation of key national cyber security stakeholders, including government representatives, private sector, civil society and academia. Facilitated by OAS experts, sessions first seek to familiarize participants with the purpose of national cyber security strategies, and to introduce them to the function and components of a number of strategies that are in effect around the world. Following the roundtable discussions, the OAS compiles and organizes the information gathered and submits a comprehensive draft strategy to Member State point of contact, who then circulates it to the wider national cyber security community. A process of feedback and revision facilitated by the OAS then begins, which continues until the Member State's needs are met and the document is considered final and submitted to the appropriate authorities for approval.

The OAS has helped Colombia (2011), Panama (2012), Trinidad and Tobago (2013), and Jamaica (January 2015) develop and adopt national cyber security policy frameworks. The OAS is also working with Dominica, Suriname, Costa Rica and Peru, on the development of their respective national cyber security strategies.

## 2. CYBER SECURITY TRAININGS AND WORKSHOPS

Based on country-specific needs and requests, the OAS provides trainings geared to officials with direct responsibility – supervisory or technical – for securing or coordinating national cyber security. These training activities target a broad audience of cyber security actors, including law enforcement agents, incident response and technical personnel, private sector stakeholders, policymakers, among others.

On average, the OAS Cyber Security Program provides training to more than 1200 officials per year. The delivery of technical training to officials has proven to be a highly successful mean of enhancing cyber security at the national and regional levels, and of building networks and confidence among participants. The OAS Cyber Security Program has offered training on advanced industrial control systems, international diplomacy in cyber security, critical infrastructure protection, ISO 27001 Information Security Management, investigative practices, forensics, incident response, CSIRT development and management, and other cyber security related issues.

## 3. CSIRT DEVELOPMENT AND HEMISPHERIC NETWORK

The establishment and development of national Computer Security Incident Response Teams (CSIRTs) are top priority to the OAS, which promotes and offers technical assistance to these ends. The OAS Cyber Security Program has also been developing a virtual hemispheric network of CSIRTs, which seeks to facilitate real-time communication and information-sharing between CSIRTs in the Americas, as well as to ensure that each country has a designated official point of contact for cyber incident response issues.

The OAS promoted and supported the creation of CSIRTs, whose numbers rose from 4 to 18 in the last decade. The OAS is joining the GFCE CSIRT Maturity Initiative. In addition, the Cyber Security Program is currently developing a CSIRT Best Practices Guide.

## 4. CRISIS MANAGEMENT EXERCISES

By utilizing a state-of-the-art mobile cyber laboratory, the OAS conducts cyber security crisis management exercises tailored to Member State needs. This lab allows the OAS to hold exercises anywhere regardless of the quality of infrastructure or the level of connectivity, thus overcoming potential limitations that could inhibit the successful implementation of such an exercise.

The mobile cyber lab has been used for 8 national and 2 regional crisis management exercises since 2012. These drills bring together a variety of national stakeholders and international CSIRTs to enhance coordination and communication on cyber security incident handling.

## 5. AWARENESS RAISING

A two-pronged approach is employed to cyber security awareness raising campaigns: provision of tangible products (e.g., conferences, videos, posters) on the one hand, and assistance to countries in the development of a national cyber security awareness campaign on the other. The OAS has also partnered with a number of civil society organizations that specialize in reaching end users and creating awareness to assist Member States in the development of their campaigns.

The OAS Cyber Security Program is developing a cyber security awareness raising toolkit (a sort of how-to guide) to assist countries in the formulation of their own cyber security awareness campaigns focused on Internet end-users. Our partners include the Anti-Phishing Working Group (APWG) and the STOP.THINK.CONNECT. Messaging Campaign, among other civil society organizations.

## 6. CYBER SECURITY TECHNICAL ASSISTANCE MISSIONS

On a state-by-state basis, the OAS Cyber Security Program responds to countries' requests by developing and carrying out tailored technical assistance missions designed to address specific cyber security concerns. These can take a variety of formats, depending on what particular facet of cyber security a Member State wants to address. Some technical assistance missions take the form of task forces with cyber security experts; others are emergency-based assistance.

The OAS has conducted technical assistance missions in more than 10 countries in 2014 alone. For instance, in 2014 the Government of Colombia approached the OAS to organize an International Commission of Experts to assess the country's current status on cyber security. The assessment included site visits, policy, legal and institutional frameworks reviews, and ended up with recommendations provided by the experts, delivered to Ministers and other high senior Colombian government officials. In another case, the OAS deployed a team of incident response experts to Jamaica to provide cyber security incident management support, which involved cooperation from the Hemispheric Network of CSIRTs of the OAS.

## 7. ACCESS TO CYBER SECURITY EXPERTISE

By partnering with a number of international cyber security experts, the OAS Cyber Security Program facilitates Member States' access to reputable and internationally recognized expertise in different fields of information security. Through these partnerships, OAS Member States receive assistance at no cost in the formulation, implementation and technical review of their cyber security policies, and have access to a wide range of best practices, experiences and technical training activities on cyber security topics.

The OAS provides access to cyber security experts through partnerships with private sector companies (eg. Microsoft, Trend Micro and Symantec), Academia (eg. University of Oxford), and nonprofit organizations, such as the World Economic Forum (WEF), the Latin American and Caribbean Network Information Center (LACNIC), and the Internet Corporation for Assigned Names and Numbers (ICANN). These partnerships have resulted in fruitful and tangible results, such as the production of formal reports and the organization of several joint-initiatives (e.g., training activities, workshops, roundtables).

## 8. CYBERSECURITY AND E-GOVERNMENT FOR EFFECTIVE PUBLIC MANAGEMENT

Based on horizontal cooperation, strategic alliances and the efficient use of Information and Communication Technologies (ICTs) at the national and local levels, the OAS E-government program is the clearinghouse of the Americas for the promotion of electronic governance in the hemisphere through initiatives such as the Latin American Initiative for Open Data (ILDA), the Online Training Platform (OAS Virtual Campus), MuNet (Transparent and Efficient Municipalities), the Network of e-Government Leaders of Latin America and the Caribbean (Red GEALC), the Inter-American Network on Government Procurement (INGP) and the Cadastre initiative. The OAS Cyber Security Program works closely with the OAS E-government Program in the promotion of cyber security initiatives in the Americas.

The e-Government Program is focal point for capacity building, dialogue and e-Gov policy, it serves as the Technical Secretariat of RedGealc, has more than 20 different online courses available; has provided training to more than 14,000 public officials, including the organization of 15 e-Government Workshops (targeted to over 550 Mayors and municipal representatives). It has also supported the modernization of cadastre in the Caribbean, specifically in Antigua and Barbuda, and St. Kitts and Nevis under a private-sector partnership model.

## 9. IDENTIFICATION AND ADOPTION OF TECHNICAL STANDARDS FOR A SECURE INTERNET ARCHITECTURE

An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry. Security capabilities in computer products are crucial to the overall network security, and must be developed in a manner that promotes the integration of acceptable security capabilities into the overall network architecture.

To achieve such integrated, technology-based cybersecurity solutions, network security should be designed around international standards developed in an open process. The development of standards for Internet security architecture will require a multi-step process to ensure that adequate agreement, planning, and acceptance are achieved among the various governmental and private entities that must play a role in the promulgation of such standards.

# HOW WE DO OUR WORK

## STEP ONE: MEMBER STATE REQUEST

The Organization of American States (OAS) provides tailored technical assistance and delivers cyber security capacity building initiatives upon request from Member States. The request for assistance can be made through the Member State's National Point of Contact, or through a simple email addressed to the OAS General Secretariat (cybersecurity@oas.org).

Member States are also invited to complete our "Technical Assistance Request Form" (Annex A), which is geared towards getting more specific information about the assistance requested (specific need or concern, requesting institution, target beneficiaries, expected timeframe, and resource availability). It represents a starting point for the joint identification, where possible, of relevant expertise and resources to meet the current and future cyber security needs of requesting institutions.

## STEP TWO: CONSIDERATION OF THE REQUEST BY THE OAS

Each request for technical assistance is closely examined by the OAS General Secretariat, taking into account the information provided by the Member State, as well as the availability of personnel, current work program, and financial and in-kind resources to undertake the proposed initiative.

Together with the country's government representatives, the OAS evaluates the cyber security needs and, based on such results, plans of action are made for strengthening cyber security capacities in the country.

If the OAS General Secretariat does not have sufficient financial resources available to deliver the requested support, it may design, in consultation with the requesting Member State, a funding proposal to be submitted to various donors. The OAS may also use the platform offered by the Global Forum on Cyber Expertise (GFCE) to assess the interest of potential donors in supporting the initiative.

## STEP THREE: DESIGN

In order to identify and understand a country's specific challenges, the OAS initiates the design process by conducting a situational analysis. This may entail in-situ visits with Government officials and other relevant national cyber security stakeholders, including representatives of civil society, the academia, and the private sector. The design process can also entail the organization of roundtables and moderated working group discussions, the administration of surveys, and the gathering of other information needed to prepare a more detailed framework for the initiative's implementation.

Thanks to the partnerships developed over the years, the OAS works closely with a variety of experts and institutions specialized in different areas of cyber security in the region and worldwide, in the design and implementation of its supporting initiatives.

## STEP FOUR: IMPLEMENTATION

Once the OAS and key country stakeholders agree on a design, the implementation phase can start with the delivery of the project's activities. Throughout the implementation phase, the OAS monitors the delivery of the initiative through the regular gathering of information. Adjustments to the initiative can be brought based on these findings or at the request of the Member State's government.

The implementation process is usually carried out with the support of the OAS pool of experts and technical and policy actors from a wide range of sectors within the Member State.

## STEP FIVE: FOLLOW-UP MISSION AND GFCE REPORT

When the implementation phase is finalized, the OAS organizes follow-up missions to ensure that countries adopt a long-term and continuous approach to cyber security projects in the country. Follow-up missions are essential to identify Member States' progress in building cyber security capacity, and to discuss the possibility of taking a step forward towards the implementation of more advanced objectives. External evaluations may also be conducted, with the participation of all stakeholders involved, in order to assess the results achieved by the project/initiative.

At the Annual GFCE meeting, the OAS General Secretariat will present a report on projects and activities taken place in the Americas. This report will describe the results achieved and the challenges still to be addressed.

# ANNEX
# -A-

# TECHNICAL ASSISTANCE REQUEST FORM

This form is to be completed by OAS Member States interested in requesting assistance from the General Secretariat for capacity building initiatives in various areas of cyber security.

## REQUESTING MEMBER STATE AND INSTITUTION

Country: _____

Name of the institution in need of support: _____

Department/Area: _____

Contact person within the institution: _____

E-mail: _____

Telephone number: _____

## DESCRIPTION OF THE NEED

Please describe in a few words or sentences the cyber security concern/need that your country/institution is facing.

## REQUESTED SUPPORT

Please explain how the OAS General Secretariat and/or its partners can help you respond to this concern/need. You may do so by checking one or more of the following services and/or by describing the type of support requested in the text box that follows. If there is more than one area of interest to your country/institution, please indicate an order of priority, being 1 the most important.

Technical Assistance Mission:

- ☐ General needs assessment
- ☐ Provision of expertise in a specific area (please provide details below)
- ☐ Development or Modernization of CSIRT
- ☐ Development of National Cyber Security Strategy
- ☐ Cyber Security and E-Government
- ☐ Crisis Management Exercise
- ☐ Public Awareness Campaign
- ☐ Trainings (please provide details below)
- ☐ Other (s)

Possible topics include, but are not limited to: critical infrastructure protection, information security management, investigative practices, forensics, incident response, CSIRT management, etc.

Please provide details on the support requested:

## TARGET BENEFICIARIES

Who are you expecting will benefit directly from the proposed support?

## NATIONAL PARTNERS

Which other institutions have been engaged or need to be engaged (e.g., other government agencies, private sector or civil society stakeholders)?

## TIMEFRAME

When would you like to receive the proposed support? (e.g., fourth quarter of 20XX)

## RESOURCES

Are there financial and/or in-kind resources currently available within your institution to meet the aforementioned need? Have you approached some donor agencies?

## GFCE CONTACT INFORMATION

### OAS CYBER SECURITY PROGRAM

Tel. +1 202.370.4674
E-mail: cybersecurity@oas.org
Website: www.oas.org/cyber


Organization of
American States

# OAS CYBER SECURITY PROGRAM

Inter-American Committee Against Terrorism
Secretariat for Multidimensional Security

ORGANIZATION OF AMERICAN STATES

1889 F Street N.W.
Washington, D.C. 20006
P. 202 370 4674
F. 202 458 3857
cybersecurity@oas.org

# WWW.OAS.ORG/CYBER