2018 OAS – DIPLOHACK STUDENT CHALLENGE

In partnership with the General Secretariat of the Organization of American States (GS/OAS),
the Inter-American Committee against Terrorism (CICTE) and the United States (U.S.) Department of State

About the project

Background

In 2018, the OAS, with the support of the United States Department of State, will host its first DiploHack Student Challenge. The aim of the event is to strengthen the cybersecurity capacity, skills and awareness of our future leaders on pressing cybersecurity issues. Balancing national approaches and a collective crisis management response, it also aims to foster a culture of cooperation as well as a better understanding of the role of international and regional organizations in responding to serious cyber incidents. Throughout the exercise, participating teams will consider current developments relating to responsible state behavior in cyberspace and in the use of information communication technologies (ICT) during peacetime and in the context of armed conflict, the emerging body of confidence building measures to reduce the risk of conflict stemming from the use of ICT and voluntary, non-binding political norms of state behavior; the debate over how international law applies to cyberspace and questions relating to capacity to respond to ICT-related incidents.

The OAS will select **six (6) teams** to participate in the 2018 OAS DiploHack Student Challenge; four teams from Latin American and Caribbean Universities, one from an American university and one from a Canadian University.

Each team will be comprised of five students with different backgrounds (e.g., international relations, law, STEM, and security), plus one faculty advisor drawn from their current academic institution and who will serve as a mentor to the team. Students should also be able to demonstrate a strong command of written and oral English (see link to OAS criteria for language proficiency).

Successful teams will be required to have the necessary entry requirements into the United States and be available to be in-country for a period of 5 days (inclusive of travel dates and dates of the event).

Eligibility

To be considered for this opportunity, each team must:

- Submit a complete OAS-DiploHack online application with all required supporting documents; and
- Be a citizen and/or permanent legal resident of the following OAS member states:
  - ✔ Argentina
  - ✔ Brazil
  - ✔ Canada*
  - ✔ Chile
  - ✔ Colombia
  - ✔ Costa Rica
  - ✔ Mexico
  - ✔ United States*
  - ✔ The Caribbean (This includes CARICOM Member States that are part of the Organization of American States)

  * Students from academic institutions in United States and Canada are encouraged to apply but benefits will be distributed on a case by case basis

The following applicants are ineligible:

- ✘ Citizens from OAS member states not mentioned above;
- ✘ GS/OAS staff and their immediate relatives or GS/OAS consultants; and
- ✘ OAS Permanent officials and their immediate relatives.

Benefits for participation

Project	DiploHack Student Challenge
Modality	Onsite, Washington D.C., United States
Language	English
Open	August 17, 2018
Deadline	September 23, 2018
Benefits*	• Airfare (economy class). • Accommodation and/or meal costs during the days of the DiploHack. • Mentorship in cyberdiplomacy.

* Financial Support will be limited and provided on an as needed basis.

Responsability of participants

Each student and mentor, university or government is responsible for covering any additional costs not mentioned, including those listed below.

Responsability of recipients	• Health Insurance • Incidental Expense • Visa procedure to enter the United States (if applicable) • Any other related costs not listed above

The expenses listed above shall be the sole and exclusive responsibility of the participants or their supporting university or government.

Submission of applications

1. To apply for the OAS DiploHack Student Challenge, each team must fill out the OAS-DiploHack online application form and attach **ALL** required supporting documentation listed below.

2. Each team applying to the OAS DiploHack Student Challenge is required to submit the following supporting documents:

   - An **application letter** (max. 1.5 pages) outlining:
     - The five (5) team members being proposed to participate in the OAS DiploHack Student Challenge and the skills each member will bring to the team; and
     - How the combination of the team skills will contribute to the event.

   - A **short essay** (max. 3 pages) on the following topic:

     Essay question
     "What are the principal policy challenges posed by the malicious use of ICT to the Americas and how might the OAS best address them?"

   - A **one-page CV** for each of the five (5) team members and the team mentor (6 Cvs in total).

   - A **Government issued ID** of each student and mentor – e.g. scan of photo of passport page that contains the applicant's full name, date of birth, and country of citizenship.

   - **Proof of English Proficiency**, if applicable, of each student and mentor – students and mentors whose native language is not English, it will be required to submit:
     - A confirmation letter certified by your university indicating a high level of proficiency in English (written, oral and comprehension) as well as any relevant course work in English *(for students)* or as an English professor *(for mentors)* in the last two years. *Relevant coursework includes classes taken in high school, English institutes, etc.*

   - **Proof of Additional Funds** of each student and mentor – proof that the team has sufficient funds to cover remaining expenses not covered under the benefits by including one, or a combination, of the following documents with your application:
     - A sponsor letter from current university.
       - If the University will sponsor the team (students and mentor), one sponsor letter which includes the names of the students and mentor should be provided.

The Essay

3. The essay must be well-structured and should include proper citation of all sources and references. It should be prepared by the students with guidance from the team mentor. Students are not expected to be experts on digital / cybersecurity (although knowledge of these areas will certainly be of benefit).

4. The objective of the exercise is to promote critical thinking among the participating teams and for students to deepen their knowledge on issues relating to digital/cyber security and related policy, and be open to learning new topics and skills. In this regard, when approaching the essay, students are encouraged to take the following approach:

   - Spend time thinking about/de-coding the essay title.
   - Plan the essay and how to approach the different elements that need to be addressed.
   - Research the subject.
   - Consider how you want to structure the essay.
   - Develop the argument and introduce counter-arguments, where relevant.
   - Make use of relevant evidence and be sure to cite sources.
   - Ensure coherence in writing style and presentation.

NOTES:

- All documents must be in English or officially translated to English by a certified translator.
- **ALL** the required documents must be combined into **one (1) single PDF file (no larger than 5MB).** The application system does not allow for more than one document to be uploaded.
- The Dean of the university or her/his designated representative should submit the application, on the university letterhead, duly dated and stamped.
- **ONLY COMPLETE APPLICATIONS WILL BE CONSIDERED**

Click here for the online application form and list of supporting documents

Selection criteria

In an attempt to make the selection process fair and objective, OAS DiploHack Teams participants will be selected on the basis of their application package, which will be weighed against established criteria below. In this regard, each applicant university is assigned points for various components of their application, and six of the top-scoring teams will be selected to participate.

1. Evaluation scheme for the selection of teams

	Criteria	Description	Max. Points
THE APPLICATION LETTER	1.1 Team composition - students	The team draws together five students from different fields (international relations, law, STEM, security etc.);	5
	1.2. Team composition - mentor	The team mentor's profile is suitable to the tasks of providing substantive guidance and support to the students.	5
	1.3. Contribution of the team (students and mentor) to the event	The application articulates how the combined skills of the students and their mentor are expected to contribute to the DiploHack challenge.	5
	1.4 Presentation	The application letter and all accompanying documentation is submitted in accordance with the stipulated guidelines and is presented in a clear and compelling manner.	5
		TOTAL POINTS	20

2. Evaluation scheme for the selection of teams

	Criteria	Description	Max. Points
THE ESSAY	2.1 Understanding of the assignment	The essay demonstrates an understanding of the issues and correctly addresses existing and emerging policy challenges.	5
	2.2 Critical thinking	The essay demonstrates an ability to think clearly and rationally about the essay topics, the arguments are presented in a compelling way, providing references where relevant, and the overall structure is coherent.	10
	2.3 Completeness of the issues addressed in the essay	The essay addresses cybersecurity policy issues from a holistic perspective, not just from the perspective of one sector.	5
	2.4 Clarity of the recommendations	The recommendations put forward in the essay are clear and realistic.	5
	2.5 Presentation	The essay is presented in a clear and compelling manner.	5
		TOTAL POINTS	30

Selection process

Selection Committee	The OAS will select the teams based on the criteria listed above. The list of the teams will be published on www.oas.org/scholarships.
Notification of selected candidates	The OAS will contact selected teams by email with the offer to participate and instructions. Teams who are not selected will not be contacted.

Code of conduct

All participants will be required to adhere to the Code of Conduct of the Secretariat for Multidimensional Security (SMS)[1]. SMS aspires to create a working environment in which participants can share their opinions and perspectives, and fully participate in activities without fear of reprisal, intimidation or harassment. As a result, SMS expects all participants in its activities to be respectful of others and to adhere to the following rules:

- **Respect and Dignity.** SMS, in compliance with GS/OAS policies, strives for a positive professional work environment in which every participant is treated with respect and dignity. Therefore, all participants must respect personal space and common courtesy for personal interaction; refrain from making exclusionary comments, even in jest; and not address others aggressively or in a demeaning manner.

- **Harassment free environment.** All participants have the right to a harassment-free and respectful environment. Harassment is any form of unwanted and unwelcome behavior, which may range from mildly unpleasant remarks to physical violence. Harassment, regardless of its manifestation, is hurtful and interferes with another person's experience and participation in SMS activities. The SMS and the GS/OAS have a **zero tolerance** policy for harassment or any other type of unlawful discrimination.

- **Be considerate of other participants' ability to contribute to the activity**, including use of allocated time. Everyone should have an opportunity to be heard. In group sessions, please keep comments succinct so as to allow maximum engagement by all. Do not interrupt others on the basis of disagreement; hold such comment until they have finished speaking.

These rules apply to all types of activities, including social events, and are aligned with Executive Order No. 15-02, "Policy and Conflict Resolution System for Prevention and Elimination of All Forms of Workplace Harassment," a copy of which is available for your information at http://www.oas.org/legal/english/gensec/EXOR1502.htm.

Promptly report any behavior that makes you or others feel uncomfortable to GS/OAS Official. You can also report issues (even anonymously) by emailing cybersecurity@oas.org. Please use an email address where you'll be able to receive replies. Once a report has been received, GS/OAS will take all applicable steps pursuant to Executive Order No. 15-02 to ensure the issue is addressed in the most confidential and expedient matter possible.

In the event of incompliance with these rules, kindly note that SMS reserves the right to remove any participant from current or future SMS activities.

Thank you for your understanding and for your anticipated cooperation.

[1]The CICTE Secretariat is a sub-secretariat of the Secretariat for Multidimensional Security (SMS)

About the partner institutions

The General Secretariat of the OAS (GS/OAS) is the central and permanent organ of the Organization of American States (OAS). Through its Department of Human Development, Education and Employment (DHDEE), GS/OAS supports OAS member States in creating policies and executing programs that promote human capacity development at all educational levels. By enabling formative opportunities to citizens, DHDEE strengthens democratic values and security under the framework of regional integration. DHDEE does this: (i) by supporting the efforts of OAS member states to improve the quality of and equity in education; and (ii) by assisting the citizens of the Americas in realizing their full potential by giving them access to knowledge and skills through training that improves the standard of living for individuals, families and communities in the region.

The main purpose of the Inter-American Committee against Terrorism (CICTE) is to promote and develop cooperation among member states to prevent, combat and eliminate terrorism, in accordance with the principles of the OAS Charter, with the Inter-American Convention against Terrorism, and with full respect for the sovereignty of states, the rule of law, and international law, including international humanitarian law, international human rights law, and international refugee law. The CICTE, through its Cybersecurity Program, works to strengthen the capacity of member states to detect cyber threats, as well as to prevent, respond to and recover from cyber incidents, based on a multi-stakeholder approach.

In partnership with other countries, the United States (U.S.) State Department is leading the U.S. Government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To more effectively advance the full range of U.S. interests in cyberspace, the Office of the Coordinator for Cyber Issues (S/CCI) was established in February 2011. S/CCI brings together the many elements within the State Department working on cyber issues. Its responsibilities include:

- Coordinating the Department's global diplomatic engagement on cyber issues.
- Serving as the Department's liaison to the White House and federal departments and agencies on these issues.
- Advising the Secretary and Deputy Secretaries on cyber issues and engagements.
- Acting as liaison to public and private sector entities on cyber issues.
- Coordinating the work of regional and functional bureaus within the Department engaged in these areas.

Contact information

Questions about this opportunity should be sent to cybersecurity@oas.org with the subject "OAS-DiploHack Student Challenge"

For more information

Please contact: Mariana Cardona at cybersecurity@oas.org