International Civil Aviation Organization

Eighth Meeting of the Common aeRonautical Virtual Private Network Operations Group (CRV OG/8)

Video Teleconference, 17 – 19 May 2021

Agenda Item 10: Share best practices on cybersecurity and develop agenda items for joint session of ACSICG/CRV/SWIMTF on cyber safety/security and resilience

UPDATE ON ICAO APAC REGIONAL CYBERSECURITY WEBINAR

(Presented by the Secretariat)

SUMMARY

This paper presents the information about the planning of ICAO APAC Regional Cybersecurity webinar on 14 June 2021.

1. INTRODUCTION

1.1 During the twenty fourth Meeting of the Communications/Navigation and Surveillance Sub-group (CNS SG/24) of the Asia/Pacific Air Navigation Planning and Implementation Regional Group (APANPIRG), under agenda item 11: *Cybersecurity of CNS/ATM systems*, the participants recalled the regional efforts on cybersecurity issues in the past years, considering the nature of complexity and the need for inter section coordination within the APAC RO and with HQ and in relation to the Cybersecurity Action Plan and promoting similar drills in future, ICAO APAC is requested to plan a webinar on cybersecurity for the region in 2021.

2. DISCUSSION

2.1 In response to the Action Item No. 24-9 of CNS SG/24 meeting, ICAO APAC Regional Office initiated consultation with contributors to plan a webinar on cybersecurity for the Region on 14 June 2021, and a State Letter has been issued on 16 March 2021, with **Ref**.: T 8/10.28 - AP046/21 (CNS), which is provided in **Attachment A** to this paper.

2.2 The objectives of the webinar are to share the information and experience gained on cybersecurity issues of CNS/ATM systems focusing on awareness of cyber threats and safety risks, policy, procedure and innovation/technology from perspectives of regulators, Air Navigation Service Providers (ANSPs), and the users of CNS/ATM systems. The webinar is expected to discuss the cyber threats during phases of CNS/ATM system design, implementation and operation and ICAO trust framework at global, regional and national level.

2.3 With the support from various contributors, a tentative programme, as of 15 May 2021, for this webinar was prepared and provided in **Attachment B** to this paper.

2.4 Due to the restrictions of available resources and online mode, the webinar has been considered as a light version of this kind and is deemed to collect feedback for preparation of a face-to-face heavy version in 3 days for 2022.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in **Attachment A** and **Attachment B** to this paper;

b) contribute individual practice and experience to the webinar as speaker as soon as possible on protecting critical CNS/ATM infrastructure under cyber threats; and

c) discuss any relevant matter as appropriate

– – – – – – – – – – – – –

International Civil Aviation Organization | Organisation de l'aviation civile internationale | Organización de Aviación Civil Internacional | Международная организация гражданской авиации | منظمة الطيران المدني الدولي | 国际民用航空组织

Ref. : T 8/10.28 - AP046/21 (CNS) 16 March 2021

Subject: ICAO Asia/Pacific Regional Cybersecurity webinar:
"Management Framework for CNS/ATM Systems", 14 June 2021

Action Required: Reply at your earliest convenience, preferably, **before 7 June 2021**

Dear Sir/Madam,

I wish to invite your Administration to the ICAO Asia/Pacific Regional Cybersecurity webinar to be held on 14 June 2021.

This webinar is in response to the action items of the twenty fourth meeting of the communications/navigation and surveillance sub-group (CNS SG/24) of the Asia/Pacific air navigation planning and implementation regional group (APANPIRG), Action Item No. 24-9, ref. 11.14 of the meeting report, which requested ICAO APAC to plan a webinar on cybersecurity for the region in 2021. The objectives of the webinar are to share the information and experience gained on cybersecurity issues of CNS/ATM systems focusing on awareness of cyber threats and safety risks, policy, procedure and innovation/technology from perspectives of regulators, Air Navigation Service Providers (ANSPs), and the users of CNS/ATM systems. The webinar is expected to discuss the cyber threats during phases of CNS/ATM system design, implementation and operation and ICAO trust framework at global, regional and national level.

In case your State/administrations are interested to be a presenter in the webinar, please contact ICAO APAC office at email APAC@icao.int with copies to: YLuo@icao.int; snibhani@icao.int; and BSirapongkosit@icao.int with the topic and content of presentation **before 15 April 2021**. The detailed programme for the Cybersecurity webinar will be then uploaded onto the webinar webpage at ICAO APAC website https://www.icao.int/APAC/Meetings/Pages/2021-Cyber-Security-Webinar.aspx

The webinar bulletin containing administrative arrangements and some instructions/guidelines for using the Microsoft Teams platform to join webinar and pigeonhole platform for Q &A session is provided in **Attachment 1**.

2/...

Asia and Pacific Office
252/1 Vibhavadi Rangsit Road
Chatuchak
Bangkok 10900
Thailand

Postal Address:
P.O. Box 11
Samyaek Ladprao
Bangkok 10901
Thailand

Tel.: +66 (2) 537-8189
Fax: +66 (2) 537-8199

www.icao.int/apac
E-mail: apac@icao.int

I shall be grateful if you take advantage of the aforementioned webinar and nominate participant(s) to join the meeting by completing the online registration using https://www.icao.int/APAC/Meetings/Pages/2021-Cyber-Security-Webinar.aspx Alternatively, participant(s) may complete the form provided at **Attachment 2 to** this letter and forward it to this Office by e-mail at APAC@icao.int with copies to : YLuo@icao.int; SNibhani@icao.int; and BSirapongkosit@icao.int at your earliest convenience, preferably, **before 7 June 2021.**

Manjit Singh
Acting Regional Director

Enclosures:
Attachment 1 - Webinar Bulletin
Attachment 2 - Registration Form

International Civil Aviation Organization

ICAI Asia/Pacific Regional Cybersecurity Webinar: "Cyber Security Management Framework for CNS/ATM Systems"

(*Video Teleconference, 14 June 2021*)

WEBINAR BULLETIN

1. Schedule of the Webinar

1.1. The Webinar (Video Teleconference) will open at **0800 hrs. ICT (UTC +7)** on **Monday, 14 June 2021**.

1.2. The presentation sessions will be based on the programme published on ICAO APAC website on webinar webpage https://www.icao.int/APAC/Meetings/Pages/2021-Cyber-Security-Webinar.aspx.

2. Officers and Secretariat concerned with the Webinar

2.1. Secretary of the Webinar:

Mr. Luo Yi, Regional Officer CNS
Tel: +66 (2) 537 8189 Ext. 158
Fax: +66 (2) 537 8199
E-mail: YLuo@icao.int

Ms. Soniya Nibhani, Regional Officer CNS
Tel: +66 (2) 537 8189 Ext. 155
Fax: +66 (2) 537 8199
E-mail: SNibhani@icao.int

2.2. Additional secretarial and administrative support to the Webinar:

Ms. Bhabhinan Sirapongkosit
ICAO Programme Assistant
Tel: +66 (2) 537 8189 Ext. 49
Fax: +66 (2) 537 8199
E-mail: BSirapongkosit@icao.int

3. Registration of participants

3.1. Each participant should ensure that the respective State/Organization has registered the name and e-mail address of the official, nominated delegate(s) to the ICAO Secretariat, **no later than 7 June 2021**.

3.2. To ensure each participant's registration, and subsequent invitation e-mail to join the Video Teleconference sessions is correct, it is essential that each participant ensures their official registration form clearly shows their nominated e-mail address in print, or preferably typed.

3.3. In case any participants are interested to be a presenter during the webinar, they should register themselves **not later than 14 April 2021** and **shall send** their presentation(s) along with the title of presentation(s) in order to update name of presenters and their presentation(s) in the webinar program for publishing on ICAO APAC website.

3.4. ICAO **reserve the rights to accept/reject** the presentations proposed by the participants. In case the proposed topic/contents are considered not appropriate for presenting in webinar, the Secretariat will keep the participant(s) be informed.

4. Webinar materials

4.1. The Secretariat will make the Webinar materials (i.e., documentation, papers, templates, instructions, etc.) available in electronic format prior to the Webinar (Video Teleconference) on the ICAO APAC Office website (at: www.icao.int/apac > Webinars > Webinar List – 2021 > Cyber Security Webinar

4.2. Each participant should review the presentations and relevant materials prior to the commencement of the Webinar (Video Teleconference) discussion sessions.

4.3. Participants wishing to submit presentation for consideration by the Webinar must do so, by e-mail to the ICAO APAC Office at: apac@icao.int, as early as possible and in any case **no later than 14 April 2021**.

5. Joining the Webinar (Video Teleconference)

5.1. When joining the Webinar (Video Teleconference) sessions, please ensure your **microphone is muted** and **video is turned off**.

5.2. Each participant should ensure that their webinar display name reflects their respective State or Organization first, followed by their participant name, e.g., "**ICAO – LUO Yi**", "**AUS – *name***", "**Hong Kong, China – *name***", etc.

5.3. Each registered participant will receive by e-mail from the Secretariat with the "*Join Webinar*" link and appropriate instructions about one week before the Webinar (Video Teleconference) sessions.

5.4. Participants should join the Webinar (Video Teleconference) sessions approx. 10- to 15-minutes prior to the scheduled start of each session.

5.5. The Secretariat will provide participant(s) with additional information and instructions concerning the webinar and Pigeonhole application at the start of the Webinar. By using the Pigeonhole application, participants are encouraged to address question(s), answer(s) or comment(s) to the Webinar. See brief instruction of the Pigeonhole application in section 9.

6. Participants' working environment

6.1 Each participant should ensure they join the webinar from a location with minimal, or preferably no, background noise.

6.2 To minimize the potential for audio-feedback to hinder the discussions, each participant should join the webinar using a separate computer/device in a separate room/office. If sharing a single computer/device to join the webinar with fellow participant/s, please ensure that only one computer/device per room/office has its microphone unmuted and audio speaker on at any one time.

7. During the webinar

7.1. Participants are encouraged to address question(s), answer(s) or comment(s) to the Webinar by using the Pigeonhole application. See brief instruction of the Pigeonhole application in section 9.

7.2. Additional information and instructions concerning the webinar tools and applications, will be provided separately at the Webinar website and will also be explained during webinar introduction sessions.

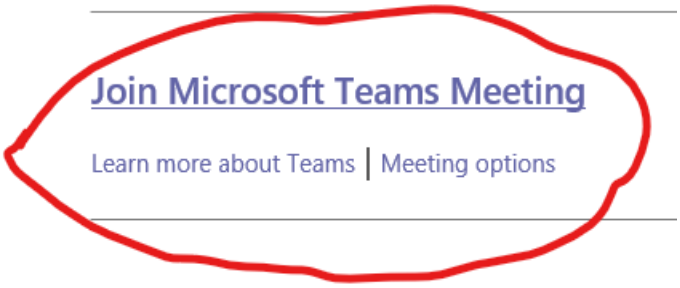
7.3. Participants should only unmute their microphone and turn on their video when invited to speak during the discussion. Please always remember to mute your microphone when finished speaking.

7.4. ICAO will manage the presentation of Webinar material during the webinar. Speakers should clearly identify to the Webinar the relevant presentation or other Webinar material they are speaking to, as well as the specific paragraphs, pages and slides, as appropriate.

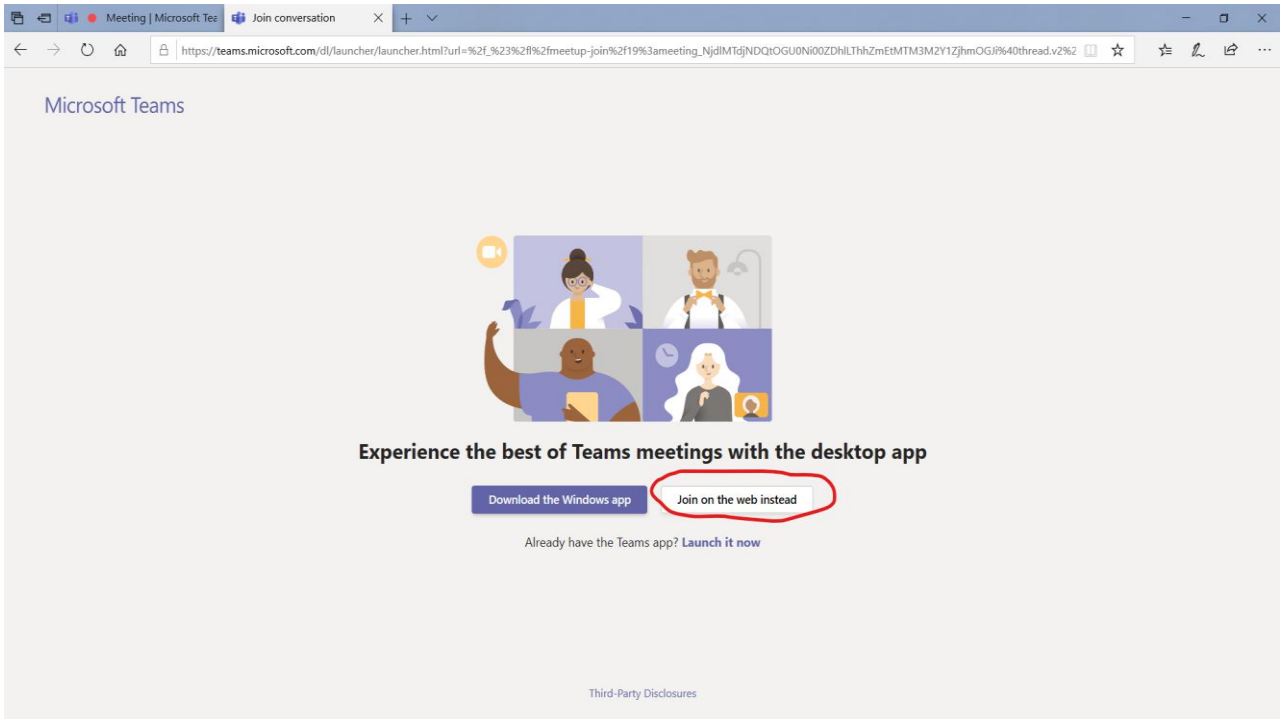
8. External User Access Guide for using Microsoft Teams

To access the Webinar as an external user, follow the steps below.

8.1 Find the email inviting you to the online Webinar, or you can check on your Outlook calendar. Click the "Join Microsoft Teams Meeting" button.

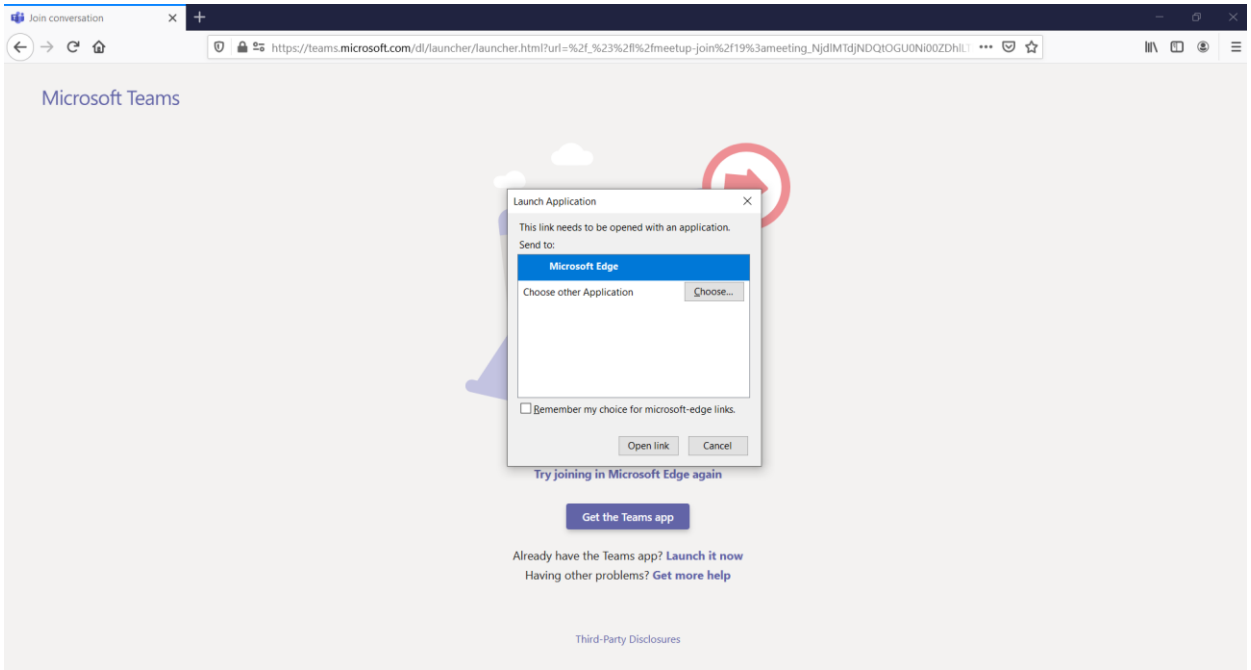


8.2 The link in the email will open the default browser on your computer. If you have the Teams application installed, you may use the "Launch it now" button. Otherwise, click the **"Join on the web instead"**, and enter your STATE or IO name first, followed by your full name (as used on the registration form) in the Enter name box. Example: ICAO Owora, Philip. Then, click join now.

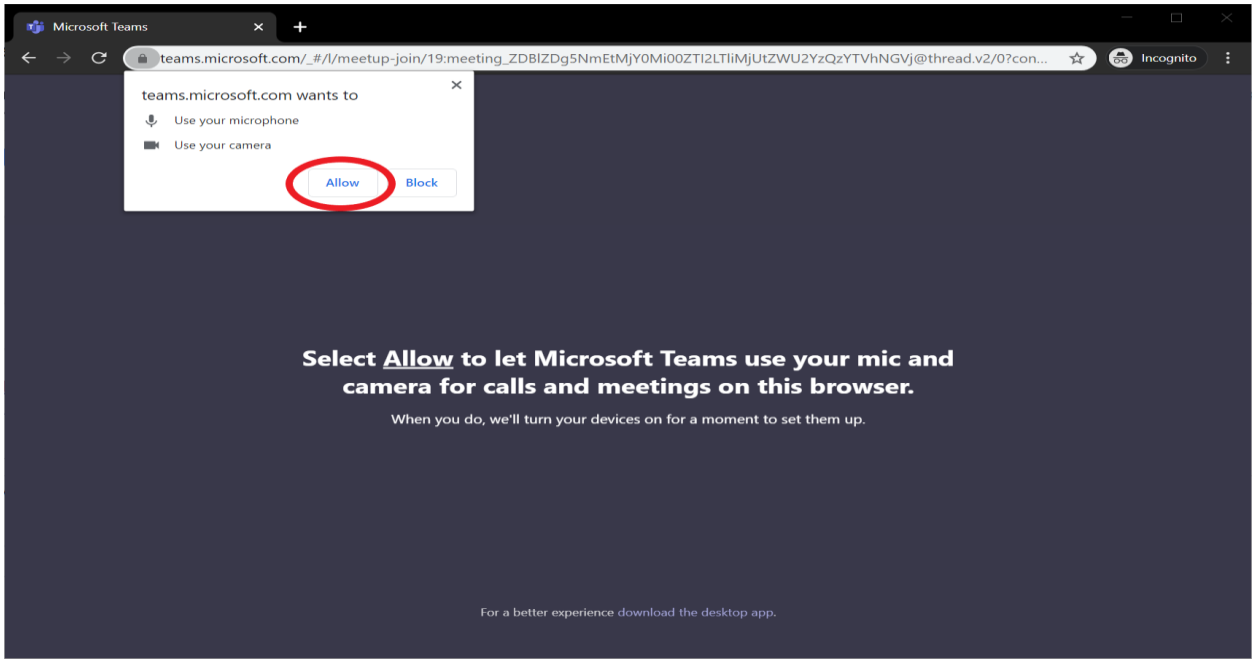


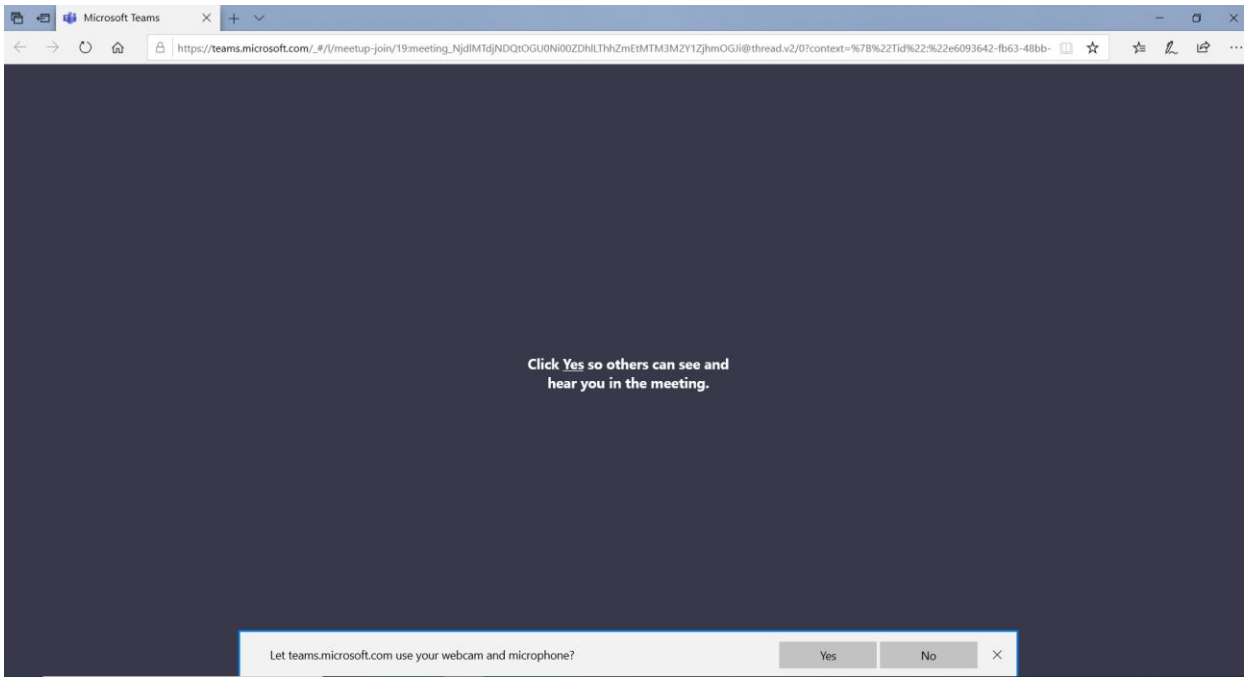
NOTE: *Some browsers are not capable of joining a Teams Webinar. Please use either Microsoft Edge or Google Chrome for the full experience. Additionally, users may "Download the MS Teams Windows Desktop app" or Mac app if they do not have Edge or Chrome.*

Select Open Link to open Microsoft Edge Browser



8.3. After clicking the Join on the web button, a new tab will appear with some basic connection instructions. Click the "**Allow**" button to let Teams access your microphone and camera.



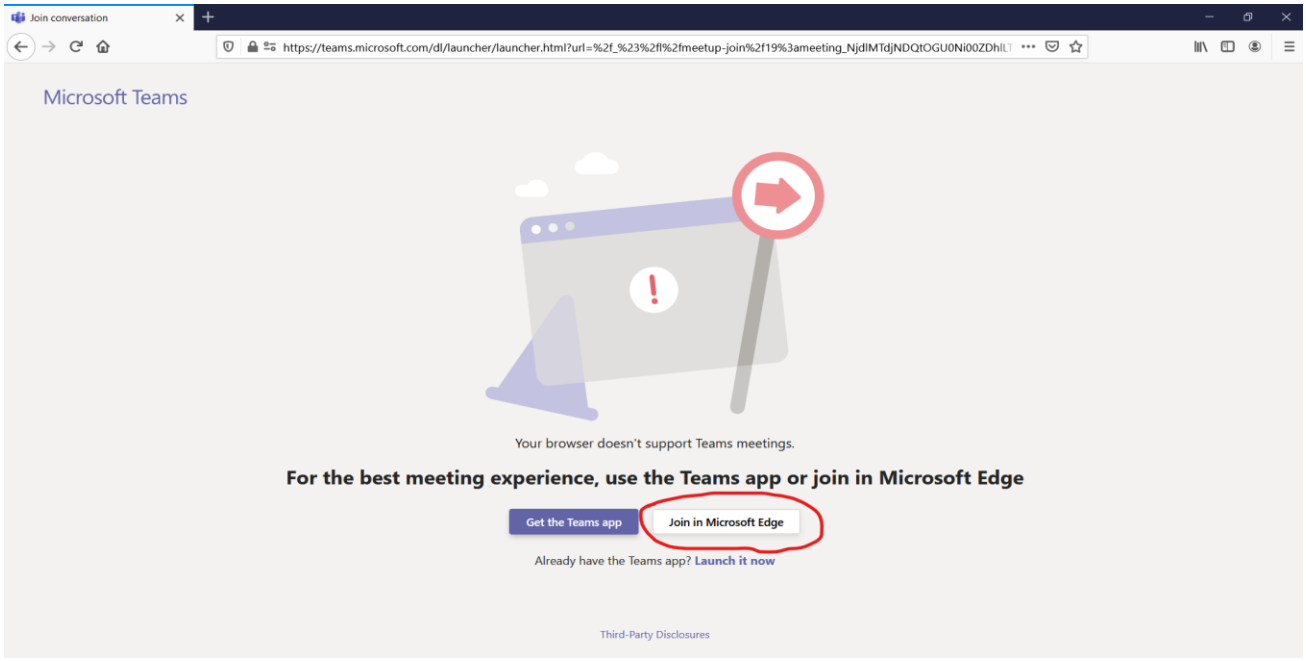


NOTE: *If you are trying to join the Webinar from an unsupported browser, you will see the following screen.*

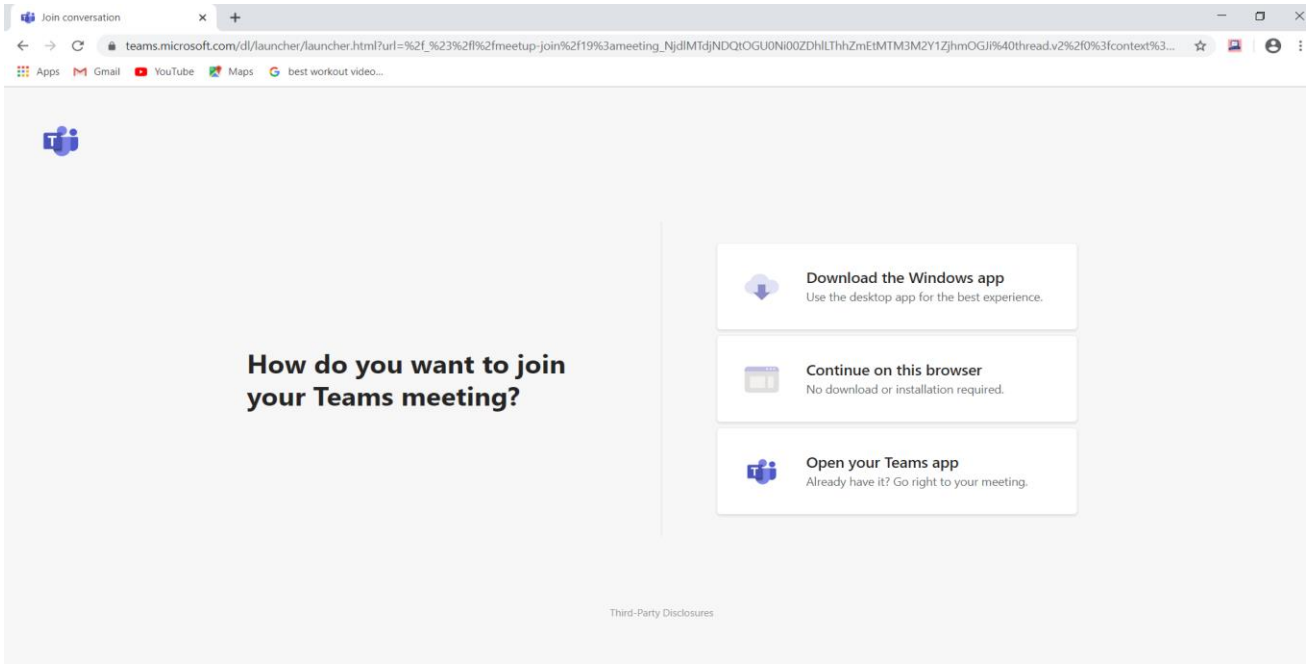
"Please use either Microsoft Edge or Google Chrome for the full experience".

Additionally, users may "Download the Windows app" or Mac app if they do not have Edge or Chrome.

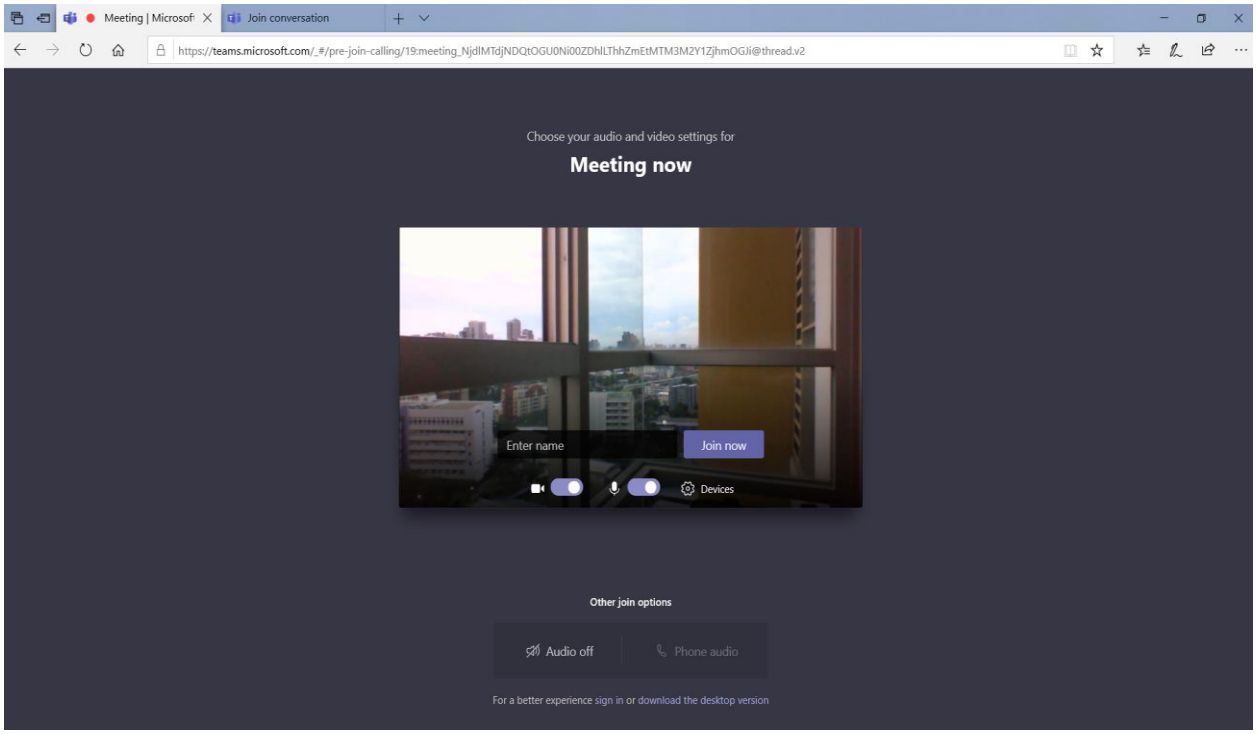
See display below when using Firefox browser



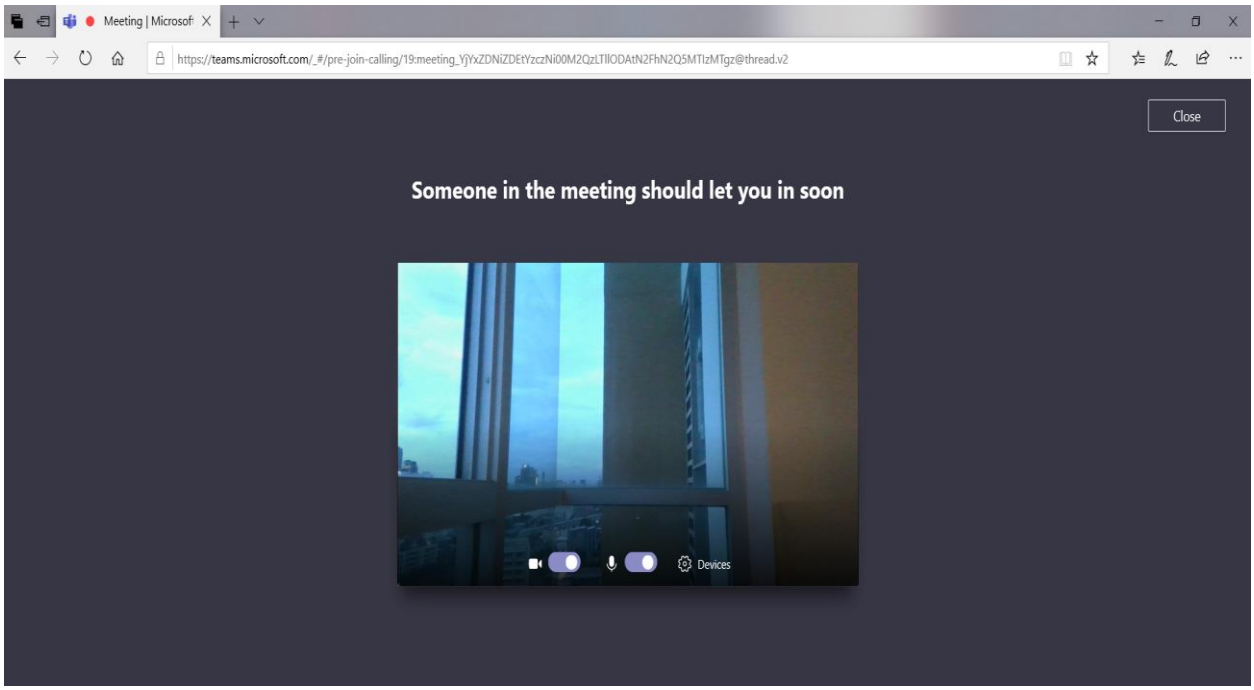
Below is displayed when using Chrome browser.



8.4 After allowing Teams access to your camera and microphone, you should now see a page with a name entry box and device options. Please enter your name and hit **"Join now"** If you do not see your camera, or it is the wrong camera, please select the **"Devices"** button to choose the correct microphone or camera.

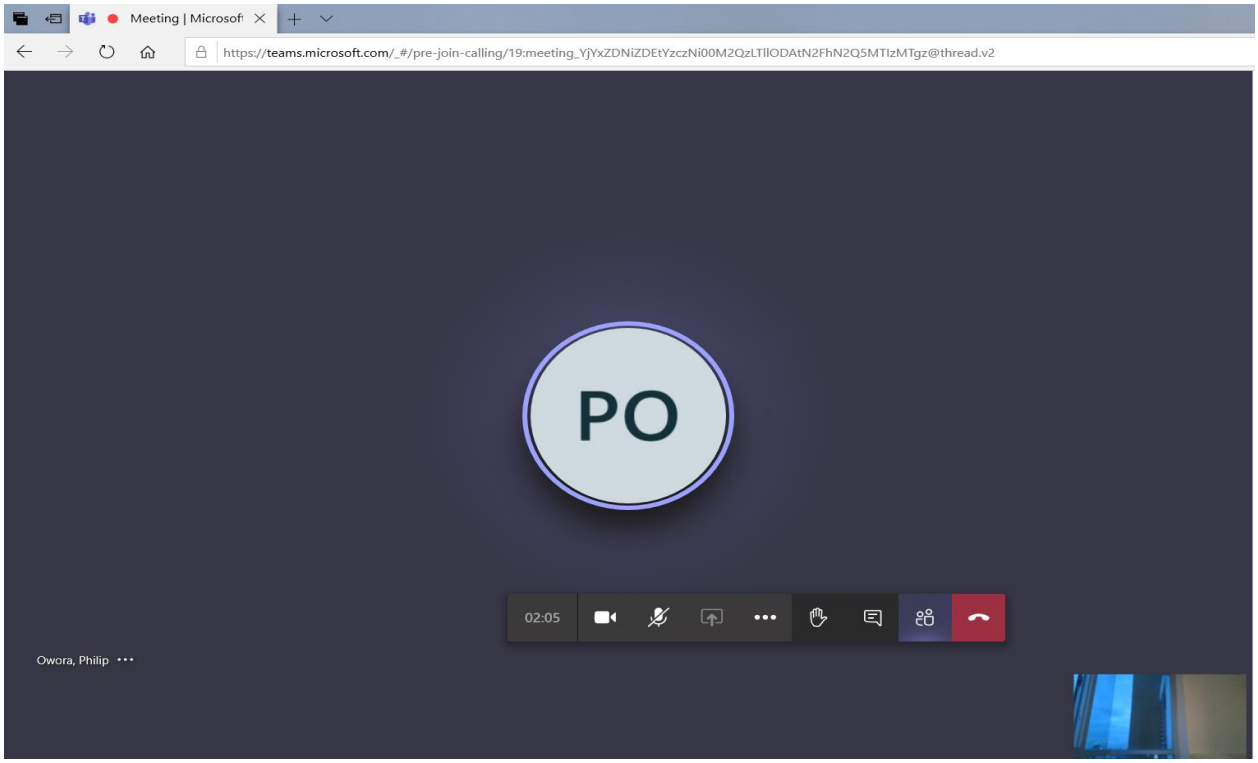


Selecting the Join now button will automatically send you into the Webinar or the Lobby where the Webinar Presenter will admit you.



Once Admitted You will be able to attend the Webinar, chat and see other participants in the Webinar.

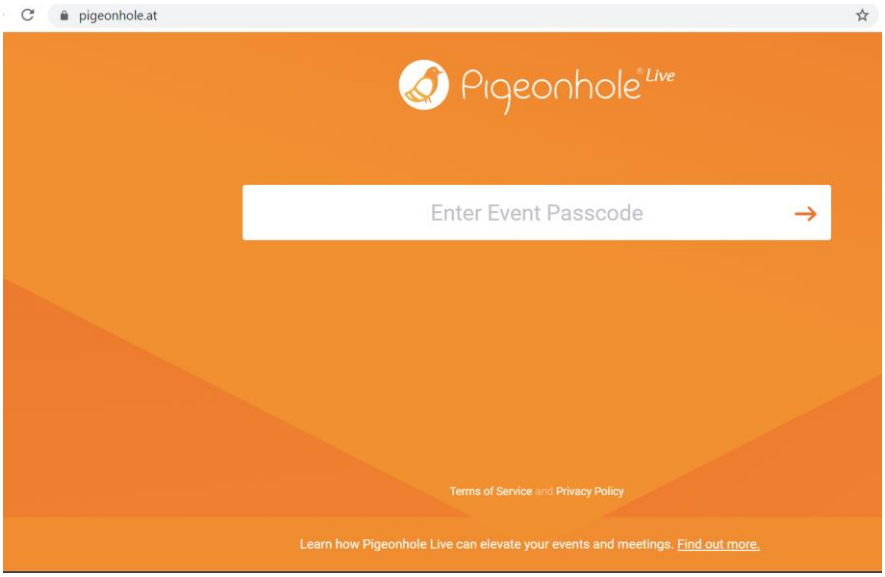
Please Sign in not less than 10 minutes before the webinar commencement time notified in the invitation email and ensure your microphone is muted and your video camera is turned off.



9. External User Access Guide for using Pigeonhole platform

9.1. Participants who attend the Cyber Security Webinar and wish to interact with the webinar with Q & A and polls, please simply use personal mobile phone and use any browser to locate https://pigeonhole.at/

9.2. Please see sample of the first page of Pigeonhole after accessing the link above. The Secretariat will provide you the password before the webinar is starting. Participants need to put the password for completely access to webpage and they will be brought to the Audience Web App.



9.3. Participants will see the agenda for the event on the Audience Web App. Participants can just tap on a session and start participating by asking questions, voting on polls, and competing in quizzes, etc.

9.4. Participants can get more information about the app, its use, and can do some practice at following link: https://pigeonholelive.com/how-it-works/#how=audience.

9.5. More information will be provided to participants during the introduction session of the webinar.

– – – – – – – – – – – –

Attachment 2 to AP046/21 (CNS)

INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

ICAO ASIA/PACIFIC REGIONAL CYBERSECURITY WEBINAR:
"Management Framework for CNS/ATM Systems"

(Video Teleconference, 14 June 2021)

REGISTRATION FORM

1. Name: _____
(☐Mr./ ☐Ms./ ☐Mrs.) **(as should appear in the official listing)**

2. Title or Official Position: _____

3. State/Administrative Region/Organisation: _____

4. E-mail: _____

Note 1: **Please download meeting materials from the ICAO APAC Office website (www.icao.int/apac > Meetings > Meeting List – 2021 > Cyber Security) prior to the meeting.**

Note 2: **Please return the completed registration form to the ICAO APAC Office (e-mail: apac@icao.int) no later than 7 June 2021**

Note 3: **Please print or type clearly. Web-conference joining instructions will only be delivered to the valid, officially nominated e-mail address/es at 4, above.**

Date_____Signature_____

After completing, please send to: ICAO APAC Office, P.O. Box 11, Samyaek Ladprao, Bangkok 10901, Thailand, or Fax: +66 (2) 537 8199 **or e-mail:** APAC@icao.int with cc: YLuo@icao.int; BSirapongkosit@icao.int

ICAO Asia/Pacific Regional Cybersecurity webinar

Management Framework for CNS/ATM Systems

14 June 2021

Opening Session	
08:00 – 08:05	**Inauguration** *Mr. Manjit Singh , Acting Regional Director*
08:05 – 08:10	**Introduction** ✓ Introduction of Participants **Logistics information** ✓ Administrative information ✓ Pigeonhole tool instructions **Please download all documents/presentations here.** **Please download your Virtual Delegate Bag here.**
Session 1	
8:10 – 09:50	**Moderator-** *Mr. LUO Yi, Regional Officer, CNS* **1. SP101 – ICAO Trust Framework Latest Development** *Ms. Olga De Frutos Martin and Mr. Michael Goodfellow* *Technical Officers, Air Navigation Capacity and Efficiency (AN), Air Navigation Bureau, International Civil Aviation Organization (ICAO)* **Abstract:** The goal of this presentation is to provide the audience with the latest updates in the International Aviation Trust Framework (IATF) being developed by ICAO. This would include updates in the information security framework as well as digital identity management system. **Question and Answer** **2. SP102 – FAA's contribution to the IATF and Importance of IATF to FAA** *Mr. Robert Segers* *NAS Information Systems Security Architect, Member of the ICAO Trust Framework Study Group, Federal Aviation Administration* **Abstract:** The goal of this presentation is to provide the audience with the latest contributions of the FAA to the validation of the International Aviation Trust Framework (IATF) as well as to highlight the importance of the IATF to the FAA. **Question and Answer**

	3. SP103 – Cyber Safety in ATM *Mr. Shayne Campbell* *Safety Programme Manager, CANSO* **Abstract:** ANSPs must be prepared to secure our systems and to adopt all necessary measures to ensure we continue to provide a highly safe and seamless air traffic services. CANSO recently launched the CANSO Standard of Excellence (SoE) in Cybersecurity, which helps ANSPs assess, develop and improve their cybersecurity in order to provide safe and resilient air navigation services. Developed jointly with ANSP and industry experts, the Standard of Excellence (SoE) contains the cybersecurity maturity model to enable an ANSP to assess its own as well as their suppliers' cybersecurity maturity. **Question and Answer**
09:50 – 10:10	*Refreshment Break + Looping Video by NOKIA*
Session 2	
10:10 – 11:50	**Moderator-** *Ms. Soniya Nibhani, Regional Officer, ANS (CNS) Implementation* **4. SP201 – Protecting All Systems** *Mr. John Moore* *Assistant Director, Safety and Flight Operations-ASPAC, International Air Transport Association (IATA)* **Abstract:** Airlines have many business, financial and administrative systems that require strong cyber protection in order to avoid disruptions. Similarly, and very importantly, airlines possess, utilise and rely on many Communications / Navigation / Surveillance and ATM systems to conduct business safely. Cyber-security must be broad and reliable so as to protect all systems and the data they use and share. **Question and Answer** **5. SP202 – DNS Ecosystem Security** *Mr. Champika Wijayatunga* *Technical Engagement Manager – Asia Pacific, Internet Corporation for Assigned Names and Numbers (ICANN)* **Abstract:** The Domain Name System (DNS) is a critical part of Internet infrastructure. This presentation will provide an overview of the DNS Ecosystem, various threats and abuses in the DNS and the best practices in protecting the DNS. **Question and Answer** **6. SP203 – Building Mutual Trust Infrastructure Based on Block Chain** *Mr.Leng Bing* *Principal Researcher, Southwest Communications Institute of China* **Abstract:** This presentation proposes a method of building mutual trust among states in the Asia Pacific region by using block chain technology, which may solve the problem that there is no trusted third party under the current global governance framework. **Question and Answer**

ICAO Asia/Pacific Regional Cybersecurity webinar

Management Framework for CNS/ATM Systems

14 June 2021

11:50 – 12:50	*Lunch break*
Session 3	
12:50 – 14:30	**Moderator-** *Ms. Soniya Nibhani, Regional Officer, ANS (CNS) Implementation* **7. SP301 – A proactive and systematic approach in protecting digitized air traffic services against cyber threats in Hong Kong from ANSP and regulatory perspective** *Mr. Raymond Chan* *Senior Electronics Engineer, Civil Aviation Department (CAD), Hong Kong, China* **Abstract:** The topic will cover the cyber security/resilience measures that Hong Kong CAD has practiced for highly digitized air traffic services systems from both service provider and regulatory perspective. **Question and Answer** **8. SP302 – Air Traffic Management Security and Updates on ICAO Cybersecurity Activities** *Mr. Remington Low* *Regional Officer FAL, Asia/Pacific Regional Office, International Civil Aviation Organization (ICAO)* **Abstract:** This presentation informs on ICAO security requirements on Air Navigation Service Providers (ANSP) and Air Traffic Management (ATM) and provides an overview on the update of the Cybersecurity Action Plan and on work undertaken by the Secretariat Study Group on Cybersecurity. **Question and Answer** **9. SP303 – A Security Solution for Information Services in SWIM** *Mr. Tian Yungang* *Section Chief, State Key Laboratory of Air Traffic Management System and Technology , China* **Abstract:** The presentation introduces the security architecture of SWIM information services, and proposes information security measures from the aspects of authentication, authorization, and information verification to improve the security assurance capabilities of SWIM information sharing. **Question and Answer**
Closing Session	
14:30 – 14:40	**10. Review Outcomes from Webinar and Closing Remarks** *Mr. LUO Yi* *Regional Officer, CNS*

NOTE: This tentative programme is subject to change.