APCICT
Asian and Pacific Training Centre for Information and Communication Technology for Development
ESCAP

Training on Cybersecurity for policymakers and civil servants

24-25 March 2026, Yerevan

BACKGROUND

In an era of rapidly advancing digital technologies, countries are increasingly exposed to a wide range of cybersecurity threats, including cyber intrusions, cybercrime, and cyber-terrorism. These threats pose significant risks to national security, economic stability, critical infrastructure, and the protection of personal data. Many countries, however, continue to face challenges in developing the institutional capacity, legal frameworks, and technical expertise required to effectively prevent, detect, and respond to such risks. Strengthening national cybersecurity governance through comprehensive policies, strategies, and coordinated institutional mechanisms has therefore become a critical priority.

Against this backdrop, the training is jointly organized with the Ministry of High-Tech Industry of the Republic of Armenia to enhance the knowledge and capacities of policymakers and civil servants in the field of cybersecurity. The programme aims to strengthen participants' understanding of key concepts related to information security and data protection, raise awareness of emerging cyber threats, and support the assessment of existing national policies against international good practices and standards. It also seeks to build participants' capacity to formulate, implement, and recommend effective cybersecurity and information security policies that contribute to a safer and more resilient digital environment.

LEARNING OUTCOMES

At the end of the programme, participants are expected to:

- Define information security, privacy and related concepts;
- Identify threats to information security;
- Assess existing information security policy in terms of international standards of information security and privacy protection; and
- Formulate or make recommendations regarding information security policy that would be appropriate to their countries.

RESOURCE PERSON

Mr. Freddy Tan is the Managing Director of EPIC Cybersecurity, a Singapore-based cybersecurity firm. He holds a Master of Science in Information Systems Security from the London School of Economics & Political Science and is a long-standing Certified Information Systems Security Professional (CISSP). With a distinguished career spanning over 25 years, Mr. Tan began his work in cybersecurity with Singapore's Ministry of Defence, where he established the 24/7 Computer Security Monitoring & Investigation Centre (COSMIC) and the Computer Emergency Response Team (SAFCERT). He has also held senior leadership roles in industry, including with Singtel, StarHub, and Microsoft, and is recognised for his contributions to the profession with honours such as the $(ISC)^2$ President's Award and Singapore's Long Service Medal (Pingat Bakti Setia). Mr. Tan is active in the professional community and has served as a founding member and committee leader in regional cybersecurity associations.

Participants

This training targets officials involved in national cybersecurity strategies, digital government, and IT and network security officiers within the Ministry and affiliated agencies.

CONTACTS

- Ms. Nuankae Wongthawatchai, Programme Management Officer, APCICT/ESCAP, wongthawatchai@un.org

PROGRAMME

Time	24 March 2025 (Tuesday) Day 1
09:00 - 09:30	**Opening Session** • Representative from Ministry of High Tech Industry • APCICT/ESCAP **Group Photo**
09:30 - 10:45	**Session 1: Need for Information Security** • Explain the concept of information and information security; and • Describe standards applied to information security activities
10:45 - 11:00	*Coffee Break*
11:00 - 12:30	**Session 2: Information Security Trends and Directions** • Provide an overview of threats to information security; and • Describe countermeasures against such threats
12:30 - 13:30	*Lunch Break*
13:30 - 14:15	**Session 3: Information Security Activities** • Give examples of information security activities of various countries to serve as a guide in information security policymaking; and • Highlight international cooperation in implementing information security policy

14:15 – 15:00	**Session 4: Information Security Methodology** • Describe internationally used administrative, physical and technical information security methodology
15:00 – 15:10	*Coffee Break*
15:10 - 16:00	**Session 5: Group discussion**

Time	25 March 2026 (Tuesday) Day 2
9:00 - 10:30	**Workshop** • Provide an overview of deepfake threats • Give examples of information security activities of various countries on deepfake countermeasures to serve as a guide in information security policymaking; and • Describe countermeasures against deepfake threats
10:30 - 10:40	*Coffee Break*
10:40 – 11:30	**Session 6: Protection of Privacy** • Trace changes in the concept of privacy • Describe international trends in privacy protection; and • Give an overview and examples of Privacy Impact Assessment
12:30 - 13:30	*Lunch Break*
13:30 - 14:30	**Session 7: CSIRT Establishment and Operation** • Explain how to establish and operate a national Computer Security Incident Response Team (CSIRT); and • Provide models of CSIRT from various countries

14:30 - 14:40	*Coffee Break*
14:40 - 15:30	**Session 8: Lifecycle of Information Security Policy** • Give an overview of the information security policymaking process; and • Discuss issues that policymakers must consider in information security policymaking.
15:30 – 16:00	**Closing**