



PROJECT NOTIFICATION

Ref. No.: 21-IP-02-GE-WSP-A-PN2100053-001

Date of Issue	14 July 2021
Project Code	21-IP-02-GE-WSP-A
Title	Workshop on Cybersecurity and Network Resilience Approaches for Industry 4.0
Timing and Duration	7–9 September 2021 (three days)
Hosting Country(ies)	Malaysia
Modality	Digital Multicountry
Implementing Organization(s)	Malaysia Productivity Corporation and APO Secretariat
Participating Country(ies)	All Member Countries
Overseas Participants	19
Local Participants	12
Qualifications of Participants	Policymakers and government officials; representatives of local government units; and staff of government enterprises, public-sector organizations, and industry representatives working on Industry 4.0 promotion, cybersecurity systems, IT governance/management, and public regulations on information systems and ICT
Nomination of Participants	All nominations must be submitted through National Productivity Organizations of member countries
Closing Date for Nominations	12 August 2021

1. Objectives

- a. Learn about the fundamentals of cybersecurity and network resilience approaches in relation to Industry 4.0.
- b. Share cybersecurity frameworks of governments to strengthen good IT governance for Industry 4.0.
- c. Understand the regulatory requirements for harmonizing security standards for Industry 4.0.

2. Background

The Fourth Industrial Revolution (Industry 4.0) is taking digital technology to the next level with the help of interconnectivity and access to real-time data, bringing a comprehensive approach to digital transformation. This truly revolutionizes how technologies allow businesses across all industries to work smarter while allocating resources for cost-effective, efficient processes. However, according to a 2019 report by the European Union Agency for Network and Information Security (ENISA) on Industry 4.0 Cybersecurity: Challenges and Recommendations, tapping the maximum benefits of this interconnectivity of things is also closely associated with ensuring cybersecurity. The report highlighted a rapidly increasing number of Industry 4.0 cybersecurity incidents, stressing the need to strengthen cyber resilience.

The need to improve cybersecurity is even more profound now since the potential impact of relevant threats ranges from compromising physical security to production downtimes and from spoilage of products to damaging equipment as well as ensuing financial and reputational losses. During the COVID-19 pandemic, industries, public services, healthcare, and social interactions, among others, have become more dependent on digital infrastructure and online information.

The APO Vision 2025 aims to support and equip the public sector as well as industry players in benefiting from the advances of Industry 4.0. The main contents of these capacity-enhancing initiatives focus on technological, digital-based learning and applications in terms of interconnectivity, automation, machine learning, real-time data, etc. to improve efficiencies and help organizations grow in the long run. In the digital transformation process to Industry 4.0, cybersecurity efforts for effective, efficient exploitation of IT solutions and critical infrastructure are needed to optimize the benefits, while overcoming cyberthreats to systems and providing countermeasures that enhance network resilience.

This workshop therefore aims to acquaint participants with the fundamentals and implications of cybersecurity and network resilience in relation to Industry 4.0, introduce relevant approaches and techniques under the good IT governance model, and provide an understanding of the regulatory requirements for harmonizing standards with Industry 4.0.

3. Scope, Methodology, and Certificate of Attendance

The duration of each day's sessions will be around three hours comprising presentations by experts, group discussions, and other relevant learning methods. The indicative topics of the presentations are:

Day 1:

- Understand Industry 4.0 and cybersecurity
- Resiliency and agility approaches for Industry 4.0

Day 2:

- Cybersecurity frameworks of governments for Industry 4.0
- Promotion of cross-functional knowledge of IT and operational technology security
- Group exercise and discussion

Day 3:

- Economic and administrative incentives for Industry 4.0 security
- Regulatory requirements to harmonize security standards for Industry 4.0

The detailed program and list of speakers will be provided two weeks prior to the sessions with announcement of the names of the selected participants.

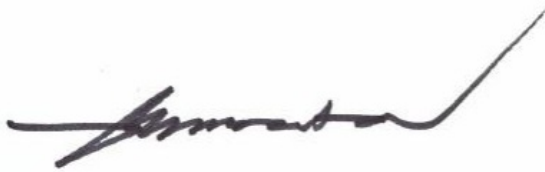
The participants are required to attend all sessions. This full participation is a prerequisite for receiving the APO certificate of attendance.

4. Financial Arrangements

- a. The APO will meet the assignment costs of overseas resource persons and honorarium for up to two local resource persons.
- b. The host country will meet the costs for a virtual site visit(s), either broadcast live or recorded as applicable.

5. Implementation Procedures

Please refer to the implementation procedures for APO digital multicountry projects circulated with this document.

A handwritten signature in black ink, appearing to read 'Mochtan', with a long, sweeping flourish extending upwards and to the right.

Dr. AKP Mochtan
Secretary-General