APPLICATION GUIDELINES for the

JP-US-EU Industrial Control Systems Cybersecurity Week

for the Indo-Pacific Region 2024

July, 2024

1. TRAINING PROGRAM OUTLINE:

1) Arrangement

- "JP-US-EU Industrial Control Systems Cybersecurity Week" is a one-week training program focusing on Industrial Control Systems (ICS) cybersecurity.
- The program is funded by the Ministry of Economy, Trade and Industry of Japan (METI) and the Industrial Cyber Security Center of Excellence (ICSCoE) of Information-technology Promotion Agency, Japan (IPA), with complementary funding and support from the U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS) and the European Commission's Directorate-General for Communications, Networks, Content and Technology (DG CONNECT).
- The program consists of hands-on exercises using the Japan IPA Industrial Cyber Security Center of Excellence's facilities, lectures and workshops by subject matter experts, and opportunities for networking among participants.
- The program accepts participants from organizations in Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam, Bangladesh, India, Mongolia, Sri Lanka, and Taiwan.

2) Language

- English

3) Date and Location

- Date: November 12th (Tues) to November 15th (Fri), 2024
- Location: Tokyo, Japan (in-person)
  Tentative venues are as follows.
  - Europe House (EEAS-Tokyo) (Day 1)
  - IPA Bunkyo Campus (Day 2, Day 3)
  - IPA Akihabara Campus (Day 4).

4) Costs

- No participation fee is required.

- Travel and accommodation expenses are to be paid by the applicant or the applicant's organization. However, funding for travel and accommodation is available for a limited number of participants. If the applicant requires funding to participate (if the applicant cannot participate without funding), please indicate in the application form in Section 3. APPLICATION PROCEDURE.

2. PARTICIPATION REQURIEMENTS:

1) Number of Applicants

1-2 persons per organization may apply.

2) Basic Qualifications

Applicants must meet all of the following requirements:

- Between 20-50 years of age (Applicant's date of birth should be between January 1st 1974 to January 1st 2004.),
- Can participate in English discussions (Intermediate and above)
- In good health and can participate in the four-day program in full
- Can pay for travel and accommodation fees as a general rule (see Section 1-4 "Costs" for details)

3) Technical Qualifications

Applicants must also meet the following requirements:

- Has at least one year of experience in OT or IT systems
- Has skillsets equivalent to CompTIA Security+, ITPEC Exam IP Level or equivalent. (certification not required)
- Engaged in OT system related work, especially those related to the following:

  i) Operation and security of process control networks and IT

  ii) Operation or management of Critical Infrastructure (CI) assets and facilities

  iii) CI component and software developers

4) Organization Requirements

Applicants must represent one of the following organizations from a country/region in scope*:

(i) Critical infrastructure providers, manufacturers

(ii) Government Office, or
(iii) National CSIRTs.

* Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam, Bangladesh, India, Mongolia, Sri Lanka, and Taiwan.

3. APPLICATION PROCEDURE:

Please note that submitting an application does not guarantee the applicant's participation in the program.

- Each applicant should submit the required information via the following online application form **no later than July 19th, 2024 JST**.

https://eprd.pl/en/dpa/japan/ics-cybersecurity-week-indo-pacific-region/application-form/

- Admitted applicants will be notified **by July 31st, 2024 JST**.
- Admitted applicants will be asked to submit a copy of passport for identification. Please have a valid passport in hand at the time of notification.
- Admitted applicants will be asked to answer questionnaires after the exercise.

4. HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION:

- Personally identifiable information provided by the applicant will only be used for the screening process and the implementation of the program and its related activities. It will not be used for any other purposes or beyond the scope required by laws and regulations of Japan, the US, and EU.
- Personally identifiable information provided by the applicant will be treated within METI based on rules under "the Act on the Protection of Personal Information". METI will outsource part of the operation.

5. FURTHER REFERENCE

- Last year's program (October 2023)
  "JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region" Held (meti.go.jp)

- About ICSCoE Japan
  https://www.ipa.go.jp/en/about/org/icscoe/index.html