ICS4ICS
Incident Command System
for Industrial Control Systems

ICS4ICS Exercise performed virtually in June and July 2023

Executive Summary

Brian Peterson and Mark Boddy, ICS4ICS program manager and volunteer, facilitated two ICS4ICS virtual Exercises in June and July 2023, with global participants. The exercise participants identified these recommendations:

- Ensure the ICS4ICS Exercise Hosting Guide is widely distributed to anyone hosting an exercise
    - Pre-planning is critical for a successful exercise and real incident response
- Ensure that ICS4ICS Team members have the resources (training, job aids, practice, etc.) to be able to perform during a real incident
- Add a slide to show the Planning-P STEM (Initial Response) activities early in the exercise
    - There was confusion by participants because they didn't understand how Initial Response occurred before kicking-off other exercise activities
- Publish past ICS4ICS Exercise hot-washes and distribute a link as part of the ICS4ICS Exercise invitation as pre-read
- Add information describing internal communication within the company
- Describe the coordination efforts and processes between the ICS4ICS Team and Operations Section (Computer Incident Response efforts) and with other teams
- Reduce some of the repetition of repeating the Planning P phases multiple times
    - Need the right level of repetition to help people learn
    - Taylor repetition to meet the needs of the audience based on their existing knowledge of NIMS/ICS (Incident Command System)
- The facilitator should provide instructions in general terms that people understand
    - Particularly for people who don't have Incident Command knowledge
- Facilitator should stand up and emphasize the points on the slides when exercise is in-person
    - The facilitator is an important role
- Create Cyber Insurance procedures based on input at these exercises

Other Feedback

These are other comments made by the participants:

- ICS4ICS is a great methodology with the planning phase, templates, and exercise materials
- This exercise was a lot better than last year's exercise and materials
- The NIMS/ICS methodology is the strength of ICS4ICS
    - ICS4ICS benefits from leveraging common NIMS/ICS processes that are known by people with Incident Command experience
- This ICS4ICS exercise is heavily scripted which enables everyone to play their roles easily