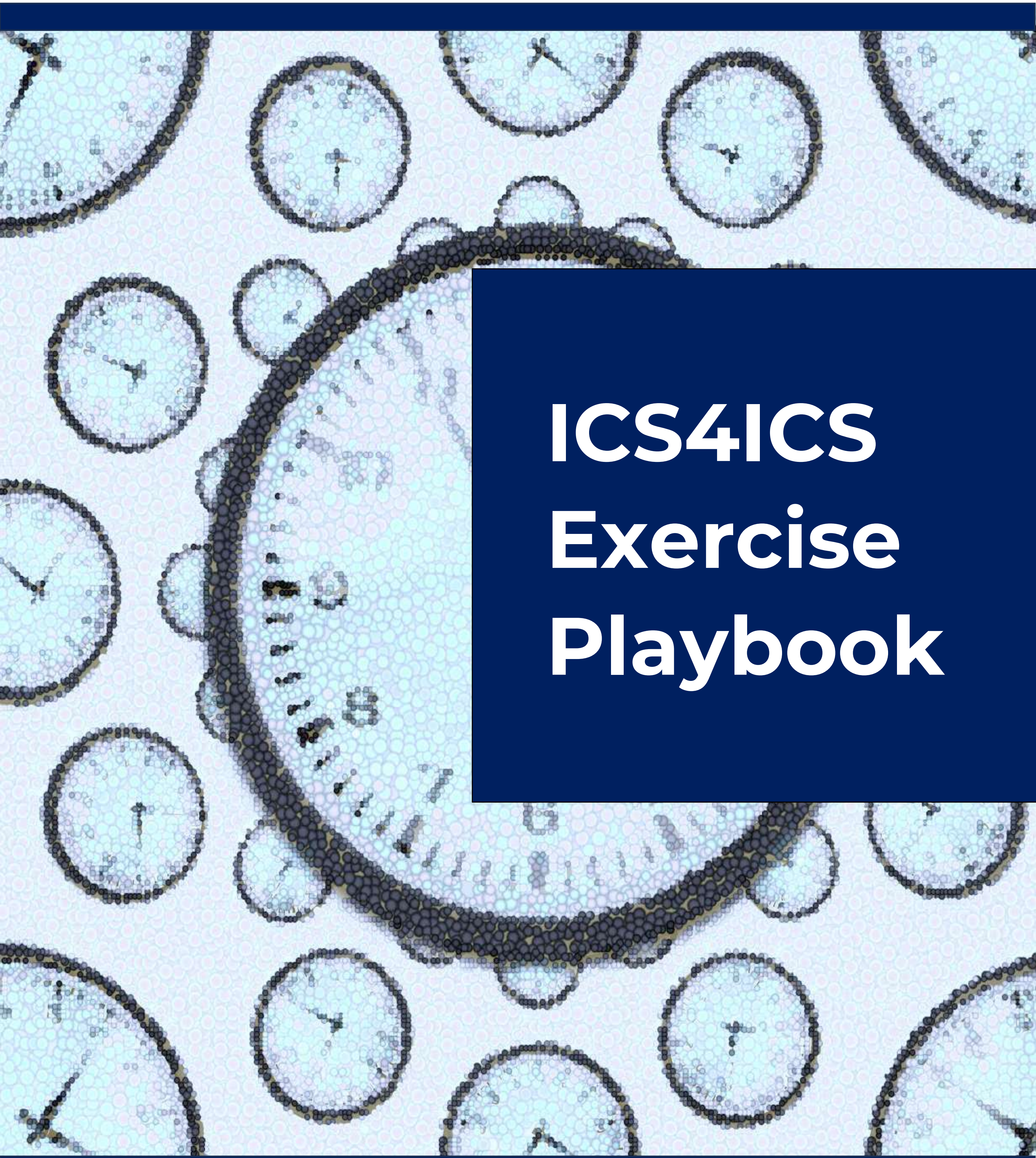
ICS4ICS
Incident Command System
for Industrial Control Systems

ISA



ICS4ICS Exercise Playbook

ICS4ICS Exercise Hosting Guide

Contents

Introduction

Purpose

This document provides information to enable a person to host an ICS4ICS Exercise.

Scope

This document is designed to help the host plan an in-person exercise. A separate document provides instructions on hosting a virtual exercise. The ICS4ICS exercises are typically 8 hours in duration. There is a shorter version, but it only demonstrates the value of ICS4ICS and is not a real exercise.

Scenario Planning

Select a scenario

Obtain input from various teams to select a realistic scenario for the exercise. Select a scenario (e.g., Hijack of the DCS HMI screen, changing process variables, causing an upset in the process) that includes a cybersecurity incident that impacts your operations (e.g., shutdown, damage). Try to select a scenario that impacts operations that exercise participants are familiar with. The complexity of the scenario should be low so that the ICS4ICS exercise participants can manage the incident.

Planning Phase: To ensure a successful outcome, it is important to devote adequate time upfront to selecting appropriate scenarios for your environment and assembling the right team. This typically takes two or three meetings. Whenever possible, involve a broad range of team members and observers in the planning process. The amount of time required for planning can differ based on factors such as team size, available resources, and the specific scenario selected. Even a planning period as short as 2 to 5 days can still yield valuable results.

Document the scenario

Document the scenario details along with a chronology of events. The document will ensure that people planning the exercise have the same understanding of the scenario.

Develop scenario injects

Define variations (injects) to the scenario used during the exercise to ensure there is sufficient complexity to the exercise and the exercise takes the full duration planned for the exercise. The ICS4ICS Team will provide an initial set of injects. The exercise presentation (PPT) has variations (injects) that should be reviewed to determine which are appropriate for your exercise.

Verify the scenario

Review with management and key leaders to verify the scenario is acceptable.

Prerequisites

Select Exercise Participants

Identify people in your company who will take a role on the ICS4ICS team in an actual incident. Determine who will play what role on the ICS4ICS Team based on management direction. This should include primary, secondary, and tertiary team members. All potential team members should obtain training and participate in an exercise. The training includes:

Course	*Course Registration*	*Prereq*	*Type of learning*	*Cost*	*Course Duration*
IS-100: Introduction to the Incident Command System, ICS-100	https://www.firstrespondertraining.gov/frts/npccatalog?id=2304	none	Distance learning	Free	2 hours
IS-700: National Incident Management System, An Introduction	https://www.firstrespondertraining.gov/frts/npccatalog?id=2404	IS-100	Distance learning	Free	3.5 hours
IS-200: Incident Command System for Single Resources and Initial Action Incidents	https://www.firstrespondertraining.gov/frts/npccatalog?id=2322	IS-100	Distance learning	Free	4 hours

These are the recommended roles to include in the exercise:

- Incident Commander (formal presentation area)
- Public Information Officer (formal presentation area)
- Operations Section Chief (area 1)
- Planning Section Chief (area 1)
- Safety Officer (area 1)
- Logistics Section Chief (area 2)
- Finance/Admin Section Chief (area 2)
- Facilitators (floats around the room)
    - Facilitator(s) will work with each group (Formal Meeting Area, Area 1, and Area 2) to help them if they have questions or need assistance completing their tasks.
- Intelligence Officer in the Operations Section
    - A person responsible for cyber threat intelligence if the company has this role.

Train Exercise Participants

Work with the ICS4ICS team members to have them complete recommended training and if possible, ICS4ICS certification. At a minimum, people who participate in the exercise should complete the first two courses required for certification. This is the email you or a senior manager from your company can send to participants:

EMAIL TO ICS4ICS EXERCISE PARTICIPANTS

You were selected to participate in an ICS4ICS Exercise to help prepare you to take a role in managing cybersecurity incidents that impact our industrial systems. Please complete these two courses to help prepare you for the exercise:

Course Description (link)	Course Registration (link)
IS-100: Introduction to the Incident Command System, ICS-100	https://www.firstrespondertraining.gov/frts/npccatalog?id=2304
IS-200: Incident Command System for Single Resources and Initial Action Incidents	https://www.firstrespondertraining.gov/frts/npccatalog?id=2322

I encourage you to obtain ICS4ICS credentials by completing additional courses defined at https://www.ics4ics.org/training

Schedule Exercise

Find a date, time, and location that works for the exercise participants. See the next section for a description of the room that is required for the exercise. Send an invitation like the following:

INVITATION TO ICS4ICS EXERCISE PARTICIPANTS

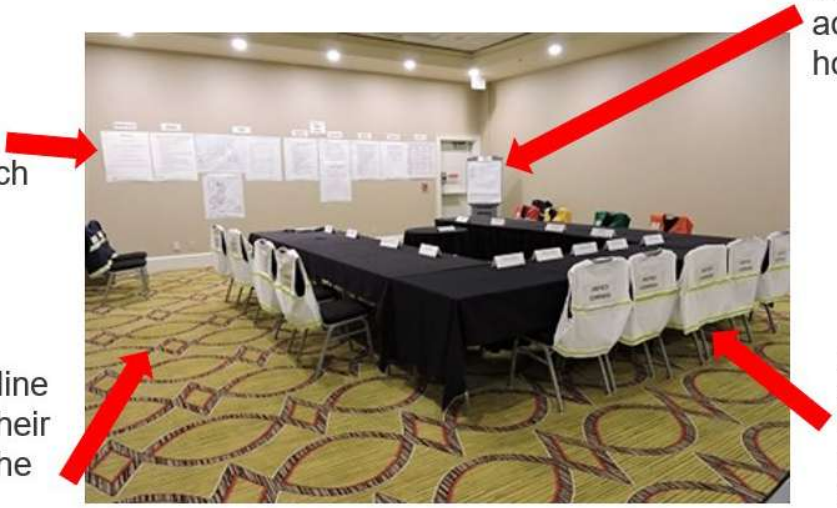
You were selected to participate in an ICS4ICS Exercise to help prepare you to take a role in managing cybersecurity incidents that impact our industrial systems. Please be prepared to spend the entire 8 hours participating in the exercise.

Prepare Facility for Exercise

Facility Layout Example

This is an example of a Meeting or Briefing Room Layout for the Formal Presentation Area

1. Visual Aids are posted on the front wall. All meetings will have a Grounds Rules and Agenda visual. The rest of the visuals are dependent on the meeting or needs of the presenters.
2. Presenters will be lined up, in order of their presentation, along the side so they can quickly move up to the front when it is time for their presentation.
3. A Flip Chart on an easel with markers at the front the room is helpful for notes and ad hoc items.
4. Attendees' roles are displayed on their seats, desk cards, or by wearing position specific vests.



Visual Aids

- Ground Rules
- Agenda
- Map/Sketch
- ICS215
- ICS215A
- Etc.

Presenters standing in line in order of their position in the agenda

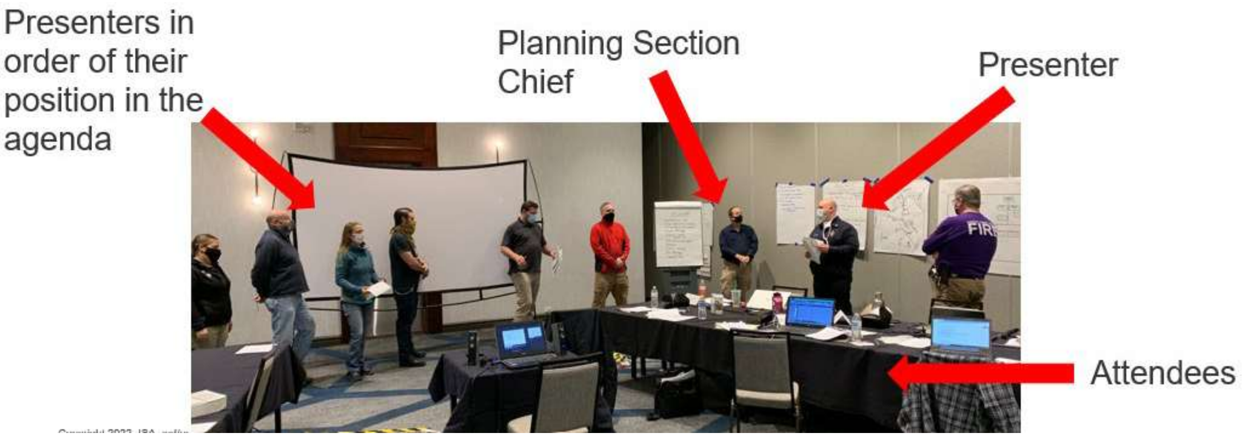
Blank pad for taking notes, additional, or ad hoc information

Attendees seated with positions clearly identified

Meeting Ground Rules (examples)

1. Silence Phones, Radios, and Pagers (UNLESS IT INVOLVES LIFE SAFETY, take it outside!)
2. No text messages or E-mail (UNLESS IT INVOLVES LIFE SAFETY, take it outside)
3. No sidebar conversations
4. Stick to the agenda
5. Presenters in Front (standing in line in the front in order of the agenda)
6. Hold Questions, Comments, & Concerns until after the meeting (except for C&G Meeting)
7. Maintain Covid Protocol *if applicable*

This picture helps illustrate how ground rule number 5 works:



Pre-Populate Forms

The exercise planning team completes these forms as pre-work before the exercise:

- INCIDENT BRIEFING (ICS 201)
- INCIDENT OBJECTIVES (ICS 202)
- ASSIGNMENT LIST (ICS 204)
- INCIDENT ORGANIZATION CHART (ICS 207)
- RESOURCE REQUEST MESSAGE (ICS 213 RR)
- OPERATIONAL PLANNING WORKSHEET (ICS 215)
- Health and safety (ICS 215A)

Select Forms to be Posted in Room

Populate the forms with data to help expedite the exercise. See the section below describing how to prepare the forms. The Planning Section Chief will post the following in the room:

- Agenda
- Meeting Ground Rules
- INCIDENT BRIEFING (ICS 201)
- INCIDENT OBJECTIVES (ICS 202)
- INCIDENT ORGANIZATION CHART (ICS 207)
- OPERATIONAL PLANNING WORKSHEET (ICS 215)
- Health and safety (ICS 215A)
- Three flip charts (blank)
    - Formal Meetings Area
    - Operations Section table
    - Planning Section table

Room Requirements

These areas are setup with a separate table or area in the room:

- Formal Meeting Area – 2 people minimum
- Area 1 – 3 people minimum
- Area 2 – 2 people minimum
- Observation Area, if desired

Areas 1 and 2 each need to be able to post four papers from their flip chart. These may be attached to the wall with tape, tacks, or magnets.

NOTE: If you are planning to have more than one person per role you will need to plan accordingly. If possible, have the primary, secondary, and tertiary person participate in the exercise as a training opportunity.

Exercise Details

Exercise Purpose

Demonstrate the ability of the ICS4ICS Team to manage an on-going, multi-operational period cyber-attack, and develop an Incident Action Plan for the next operational period. The exercise duration is 8 hours.

Exercise Objectives

These are the objectives of the exercise:

1. Train various people to fill key ICS4ICS roles: Incident Commander, Command (PIO, SOFR), and General Staff (Section Chiefs) with 1 to 3 people in each position
2. Introduce and follow the Planning "P"
3. Ensure participant understand their role and input to the Incident Action Plan
4. Enable participant to understand their roles and responsibilities by setting expectations and providing them the tools they need to be successful
5. Set expectations for team members at formal meetings

Exercise Preparation

These are steps taken prior to the exercise:

- Provide packet of resources including expectations 2 week prior to the exercise
  - ICS 201 form for initial response
  - IAP with worksheets/notes and partially completed IAP from Operational Period 2
- Meet separately with each position to review the packet and answer questions for the participants
- Identify people who have previous Incident Command Experience and have them facilitate the efforts at each of the tables
  - Meet with these people in advance to set expectations and answer questions
- Plan a follow-up meeting with key people from the exercise to help them update their materials based on learnings from the exercise AND plan next steps for future exercises

Hot-Wash (Lessons Learned)

Ensure that someone is designated to facilitate and document the Hot-Wash with lessons learned at the end of the exercise. The exercise facilitator typically facilitates the Hot-Wash. The Document Unit Leader typically records the notes during the meeting and is responsible for creating the Hot-Wash report.