ICS4ICS
Incident Command System
for Industrial Control Systems
ISA

ICS4ICS Newsletter
October 3, 2023

This is the ICS4ICS Newsletter designed to share information about ICS4ICS activities. Please reply if you have any questions or feedback.

ICS4ICS 2024 Plan DRAFT

We drafted the ICS4ICS 2024 Plan which will guide our efforts next year. We would like to receive your feedback and suggestions before finalizing this plan. We will have a series of meetings with different ICS4ICS teams to get their feedback. If you are not able to attend any of the meetings planned over the next two weeks, please share your thoughts via email. This is a high-level overview of the ICS4ICS 2024 Plan key activities:

- ICS4ICS Version 3 Exercise materials will be created in (early) 2024 to include:
    - Unified Command (UC) with a simulation of a physical incident (e.g., fire) caused by a cyber incident
    - Expand exercise to include Type 3 incidents which is a Single Company with Multiple Sites impacted
    - Industry specific ICS4ICS exercises (water, electric, etc.)
    - Cybersecurity Incident Response and ICS4ICS joint exercises
- ICS4ICS Resources will be added
    - Publish ICS4ICS Resources currently under development and continue to update them based on feedback
    - Create ICS4ICS resources to address integration between NIMS/ICS, OT/ICS, IT, and Crisis Management teams along with BCP, DR, and other processes
    - We will add resources based on feedback from the ICS4ICS members and Exercise Hot-Washes
- ICS4ICS Awareness & Outreach
    - Finalize updates to the new ICS4ICS website
    - Create informational materials including whitepapers and videos
    - Develop marketing materials that describe the value of ICS4ICS
    - Continue to identify and manage ICS4ICS Awareness & Outreach exercises, presentations, etc.

- ICS4ICS Training materials and courses
    - Partner with INL on Work Force Development (WFD) Skills Assessment to identify ICS4ICS skills and tools to assess organizational skill gaps
    - 1-hour overview of how ICS4ICS works with cybersecurity Incident Response
    - 20-minute training modules describing ICS Forms and separately Planning-P Meetings
    - 2 and 3-day course to enable participants to deep-dive into critical ICS4ICS roles and see how they work together
    - Updates Role Sheets for critical roles including liaison officers, safety roles, and others
    - Partner with other training effort (e.g., DOE CYMANII, INL ICS-301) to include ICS4ICS training in their programs

---

ICS4ICS EXERCISES

NEW Exercise Materials: We created a new ICS4ICS Hybrid Exercise that combines recorded segments (when there are not exercise players) with in-person facilitator slides and working sessions to review ICS4ICS resources (e.g., Government Reporting, Ransomware procedure, IT and OT procedures, and other documented resources).
These materials are located at: MS Teams > ICS4ICS > ICS4ICS Exercises > Files > Hybrid Exercise with video

We also updated and combined exercise materials based on the feedback we received at recent exercises: MS Teams > ICS4ICS > ICS4ICS Exercises > Files > 3-to-8-hour Exercise

- We added slides to address topics that exercise participants said would help them; we also reorganized the order of the slide based on participants' feedback

EXERCISE Completed: The following ICS4ICS Exercise have been completed since our last newsletter:

- OT ISAC Summit on Sept 6-7, 2023 (specific date to be published) in **Singapore**. Conference information: https://www.otisac.org/otisacsummit2023
- USA Colorado Incident Management Team (IMT) Conference in **Grand Junction CO** on Sept 19-20, 2023: https://dhsem.colorado.gov/2023IMTConference
- ISA Automation & Leadership Conference in **Colorado Springs, CO**, USA on Oct 6, 2023. Conference information: ISA Automation & Leadership Conference
- GridSecCon in **Quebec City, Canada** on Oct 17, 2023. Conference information: https://www.nerc.com/pa/CI/ESISAC/Pages/GridSecCon.aspx

ICS4ICS Exercise materials are posted in MS Teams:

ICS4ICS > ICS4ICS Exercises > Files > 0 Past and Future Exercise Materials > (various folders)

EXERCISE Hot-Washes: We are posting hot-wash document for these exercises when they are available in MS Teams:

ICS4ICS > Resources > Files > ICS4ICS > Hot-wash summary

ICS4ICS Credentials

NEW Credentialled Individuals: We would like to congratulate those who have obtained their ICS4ICS Credentials since our last newsletter:

- Chris Sistrunk - Incident Commander Credentials Type 4
- Matjaz Demsar - Incident Commander Credentials Type 4
- Gary Kong Wai Keat - Incident Commander Credentials Type 4
- David Jarrett - Incident Commander Credentials Type 4
- Gabriel Sanchez - Incident Commander Credentials Type 4
- Scott Johnston - Incident Commander Credentials Type 4
- Ravindra Gotavade – Operations Section Chief Credentials Type 4

The list of ICS4ICS Credentials Individuals (people) will be maintained on MS Teams:

> https://teams.microsoft.com/l/channel/19%3a5e233c34c355448e81c8ecf93fde04e7%40thread.tacv2/ICS4ICS%2520Credentials?groupId=977dda8f-3f44-4f60-b372-7eee043e8e42&tenantId=bbd40118-edcc-4393-b6ec-19ce99b81440 (select "Files" in the upper right menu bar to see the files)

ICS4ICS Credential Requirements: We published credential requirements and applications for other ICS4ICS roles including Finance/Admin, Logistics, Operations, and Planning Section Chiefs AND Public Information Officer and Safety Officer in MS Teams:

> ICS4ICS > ICS4ICS Credentials > Files > ICS4ICS Credential Applications (you will see a list of folders for each role that has ICS4ICS credentials)

NEW ICS4ICS Credentials: We are working to develop ICS4ICS Type 3 Credentials for Incident Commanders. A draft has been submitted to the ICS4ICS Adjudication Committee for their approval. We will develop ICS4ICS Type 3 Credentials for other roles. We are also adding other ICS4ICS Type 4 Credentials for common key roles typically part of the ICS4ICS Team.

ICS4ICS Training

ICS4ICS Training for Credentials: ICS4ICS credentials leverage FEMA ICS training that is required to obtain NIMS/ICS credentials. Type 4 credentials can be completed by anyone in the world through online FEMA training. The courses required to obtain ICS4ICS Type 4 credentials can be completed in 15-hours (20-hours for PIO). See our website for more information: https://www.ics4ics.org/training

NEW Training Course: We are defining the requirements for a 3-day ICS4ICS Training Course that will help students understand the activities that occur in a real cyber security incident and how ICS4ICS is used to manage these incidents.

WFD Project: ICS4ICS is partnering with Idaho National Lab (INL) on a Work Force Development (WFD) Skills Assessment project. This data and tool will enable asset owners to perform a self-assessment to determine the ICS4ICS roles that can be staffed by the organization and identify ICS4ICS roles that must be staffed by mutual aid partners. Asset owners will also be able to develop Work Force Development (WFD) plans to enable their staff to obtain competency to perform more ICS4ICS roles and obtain associated credentials. We will document the tasks for each role and then develop the WFD Skills Assessment data. We will start with Cybersecurity roles and then OT/ICS, IT, and NIMS/ICS roles.

If you are interested in volunteering to work on this project, please let me know. Brian Peterson bpeterson@ISA.org

---

ICS4ICS Resources

NEW ICS4ICS Resources: We created these new ICS4ICS resources based on input from the exercises during the last month:

- Cyber Insurance Informational resources provides information about cyber insurance and actions an asset owner needs to take when they have insurance
- Escalation-Notification-Declaration Procedure was developed and will be further refined with input from our volunteers

Updated ICS4ICS Resources: We updated the ICS4ICS resources based on feedback from the exercise that have been conducted so far:

- Ransomware Procedures provides information to help an asset owner prepare for and respond a ransomware request (the document is in the "Incident Management" subfolder)
- Government Reporting Procedure provides information about existing reporting requirements and how asset owner can prepare to make decisions during an actual incident; we are seeking input from you on other laws and regulations that should be included in this document
- Shutdown and Isolate Systems Procedure helps asset owners make decisions about protecting other systems that may be at risk from the same cybersecurity malware (this document is located in the Procedures for IT and OT subfolder)
- Problem Resolution Procedure helps asset owners identify the data they want onsite staff to collect before calling support staff to expedite problem resolution efforts (this document is located in the Procedures for IT and OT subfolder)
- We previously posted the ICS4ICS Mutual Aid resources. The Mutual Aid resource will help asset owners assess their current staffing capabilities so they can identify ICS4ICS roles that need to be sourced by a Mutual Aid (Service) provider. We will add more Mutual Aid (Service) providers to this document. Please review this resource and let me know if you have feedback or suggestions.

These resources can be found on the ICS4ICS MS Teams channel:

https://teams.microsoft.com/l/channel/19%3a5e233c34c355448e81c8ecf93fde04e7%40thread.tacv2/ICS4ICS%2520Credentials?groupId=977dda8f-3f44-4f60-b372-7eee043e8e42&tenantId=bbd40118-edcc-4393-b6ec-19ce99b81440

IN THE NEWS

These are announcements, news, and posts related to the ICS4ICS program:

REPEAT from Last newsletter: USA Public companies now have a 4-day deadline to report cyberattacks which will be effective for large companies before Year-End 2023 and small companies before end of March 2024:
SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

NEWS Articles: Articles about the SEC Reporting Requirement:
Examining the challenges with cyber incident reporting in the SEC cybersecurity rules | Energy Central
What can the Titanic Teach Us about Cybersecurity Risks and Preparations | Energy Central

---

ICS4ICS STATS

1,359 ICS4ICS members
89 countries with ICS4ICS members
All major Industry categories are represented by the ICS4ICS members
92 Sub-Industries are also represented by the ICS4ICS members
52 ICS4ICS events (presentation, exercises) were hosted this year so far this year

---

ICS4ICS Working Documents

ICS4ICS MS Teams: We created an ICS4ICS MS Teams channel that will allow us to share various materials before they are published on the ICS4ICS websites. ICS4ICS documents and resources will be published on this MS Teams channel, including Mutual Aid, Government Reporting, and IT/OT and BCP. ICS4ICS exercises materials will be shared via this MS Teams channel:

https://teams.microsoft.com/l/channel/19%3a5e233c34c355448e81c8ecf93fde04e7%40thread.tacv2/ICS4ICS%2520Credentials?groupId=977dda8f-3f44-4f60-b372-7eee043e8e42&tenantId=bbd40118-edcc-4393-b6ec-19ce99b81440

If you don't have access to the ICS4ICS MS Teams channel, please contact me: Brian Peterson bpeterson@ISA.org

NOTE: We are working to replace the current ICS4ICS website and will post the resources and others materials. MS Teams will continue to be used for working documents.