ICS4ICS Newsletter
March 23, 2024

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

The ICS4ICS volunteers were saddened to hear that Mike Chaney passed recently. We want to acknowledge his efforts as a founding member of the ICS4ICS team and his work to provide strategic leadership and on-going support of the program. Mike helped develop and played a role in our first and subsequent exercises. We will all greatly miss him.

ICS4ICS Website

NEW ICS4ICS Website: We are happy to announce that our new ICS4ICS website is available: https://www.ics4ics.org/

The new website has the information and resources that will enable the public to learn about ICS4ICS and deploy an ICS4ICS program at their companies.

ICS4ICS Events

The ICS4ICS Awareness & Outreach Team has works to identify and coordinate ICS4ICS presentations, organization engagements, and exercises. If you have any suggestions about ICS4ICS Awareness & Outreach opportunities, please contact me.

ICS4ICS Exercises: You can participate in these exercises by contacting bpeterson@isa.org

- April 10, 2024 EXERCISES
  - ICS4ICS Americas-Europe-ME-Africa Virtual exercise using ICS4ICS Hybrid exercise materials – Brian/others
  - If you haven't received an invitation and you are interested in attending, please contact bpeterson@isa.org
- April 11, 2024 EXERCISES
  - ICS4ICS Asia-Australia Virtual exercise using ICS4ICS Hybrid exercise materials – Brian/others
  - If you haven't received an invitation and you are interested in attending, please contact bpeterson@isa.org
- May TBA, 2024 - EXERCISE
  - Water Sector ICS4ICS-Cyber Incident Response Joint Exercise with Dragos – Brian/Dragos
- June TBD, 2024 EXERCISE
  - DHS CISA Region 1 'Supply Chain Forum' in MA, USA (2 hours) - Brian
- June 17, 2024 EXERCISE
  - ISA's 2024 OT Cybersecurity Summit - London, UK | ICS4ICS Workshop (all day) – Brian/Kathrine/Heidi/others
    - Obtain more info or register at ISA Conference website https://otcs.isa.org
    - Savoy Place, London, UK
    - ISA Conference: 18-19 June
- Sept 30, 2024 EXERCISE
  - ISA Automation & Leadership Conference in SC, USA (all day) – Brian/Heidi
    - Learn More
    - Francis Marion Hotel, Charleston, SC, US
    - ISA Conference: 30 September - 3 October

Other ICS4ICS Exercises and Presentations: These are the ICS4ICS Exercise planned:

- March 26-28, 2024 EXERCISES
  - Chemical (anonymous) company integrating Unified Command and Cyber Incident Response (all day) - Durgesh/Brian
- April 16 to 18, 2024 PRESENTATION
  - NATO - Critical Infrastructure Cybersecurity Workshop - U.S. Indo-Pacific Command J8 in HI, USA – Megan/Brian
- May 9, 2024 PRESENTATION
  - FIRST: Forum of Incident Response and Security Teams, virtual presentation (1 hour) - Brian
- June 9-14, 2024 PRESENTATION
  - FIRST: Forum of Incident Response and Security Teams, 36th Annual FIRST Conference in Japan – Megan

ICS4ICS EXERCISES

ICS4ICS Exercise Version 3 (2024): We created new ICS4ICS exercise materials including these additions:

- Basic ICS4ICS Exercise materials address feedback from exercise participants and includes improved formatting to make it easier to use
- Cyber Security Incident Response integrated into ICS4ICS so that participants can understand how ICS4ICS improves Cyber Incident Response efforts
- Unified Command with ICS4ICS is designed to help participants understand how to jointly manage a physical incident, like a fire, that is caused by a cyber incident

ICS4ICS Exercise V3 Next Steps: We are working to finalize the ICS4ICS exercise materials and provide complimentary resources:

- Finalize the exercise material drafts by April 1, 2024 including short videos that can be used as a hybrid exercise so participants can work on ICS4ICS procedure, like ransomware
- Host ICS4ICS In-person Exercises in Houston TX, USA before April 1, 2024 that will allow us to correct any issues we find in the exercise materials
- Host ICS4ICS Virtual Exercises by April 15, 2024 that will allow global participants to learn about ICS4ICS and participate in the development of ICS4ICS procedures, like Gov reporting
- Host ICS4ICS Joint ICS4ICS-Dragos Incident Response Exercise in May 2024 which will be an in-depth example of how ICS4ICS and Cyber Security work together
    - This exercise is focused on the Water Sector, but the lessons can be applied to any industry
- Create a 1-hour exercise video in May 2024 that can be viewed by participants before an ICS4ICS Exercise

The ICS4ICS Leadership Team would like to thank our volunteers who help create the ICS4ICS Exercise materials. The ICS4ICS Exercise Team would like to thank Jayne Lytel for her efforts that made the ICS4ICS Exercise materials look professional and ensure effective delivery of exercises, particularly virtual exercises.

If you are interested in volunteering to work on the ICS4ICS Exercise Team, please let me know. Brian Peterson bpeterson@ISA.org

ICS4ICS Credentials

The ICS4ICS Training & Credentials Team has been working to determine how we can encourage more people to obtain their ICS4ICS Credentials. We plan to setup periodic meetings to help people identify the best ICS4ICS Credential to obtain based on their experience. We also plan to help people work together to take the FEMA training required for ICS4ICS Credentials. If you have suggestions about how we can get more people engaged to obtain ICS4ICS Credentials, please let us know.

ICS4ICS Credential Completed: We would like to congratulate those who have obtained their ICS4ICS. We encourage others to complete the training and to obtain their credentials. These are the people who obtained credentials:

- Lukasz Kister , Incident Commander – Type 3
- Jon Goderis, Incident Commander – Type 3
- Matt Siomos, Incident Commander – Type 4

ICS4ICS Credential Requirements: The ICS4ICS Credential applications have been posted to the ICS4ICS website: https://www.ics4ics.org/training-and-credentials

These applications will help you understand the credential requirements for each ICS4ICS roles. If you have any questions, please contact me.

ICS4ICS Credentials Training: Most of the ICS4ICS Credentials require about 15-hours of FEMA training. The FEMA training is available free to everyone globally. The training requirements are posted on the ICS4ICS website: https://www.ics4ics.org/training-and-credentials

If you are interested in volunteering to work on the ICS4ICS Training & Credentials Team, please let me know. Brian Peterson bpeterson@ISA.org

ICS4ICS Training

The ICS4ICS Training & Credentials Team has been working on various efforts and is developing a plan to create more ICS4ICS training courses. This includes:

WFD Project: ICS4ICS is partnering with Idaho National Lab (INL) on a Work Force Development (WFD) Skills Assessment project. The data and tools will enable asset owners to perform a self-assessment to determine the ICS4ICS roles that can be staffed by their organization and identify ICS4ICS roles that must be staffed through 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 critical roles and obtain associated credentials. We have started documenting the tasks for each role and are working on developing the WFD Skills Assessment data. We have made significant progress to define jobs tasks and skills for 20+ roles in these ICS4ICS team groups: Cybersecurity, ICS/OT, IT, and NIMS/ICS roles. This Work Force Development data will be shared with NIST NICE and be used to help organizations obtain, retain, and develop staff.

NEW Training Course: We are working to draft micro training modules to explain each of the ICS4ICS procedures, templates, and other resources. 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.

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

ICS4ICS Resources

The ICS4ICS Resources have been posted to the ICS4ICS website: https://www.ics4ics.org/processes-and-tools

NEW ICS4ICS Resources: We created these new ICS4ICS resources based on input from recent exercises:

- Cyber Insurance Informational document helps assets owners decide and select cyber insurance and actions needs when a company has insurance
- Escalation-Notification-Declaration Procedure helps establish criteria for escalation with associated procedures that include how to notify staff, and incident declaration criteria

Updated ICS4ICS Resources: These are other ICS4ICS resources that were updated based on feedback from the exercise participants:

- Ransomware Procedures provides information to help an asset owner prepare for and respond a ransomware request
- Government Reporting Procedure provides information about existing reporting requirements and how asset owner can prepare to make decisions during an actual incident
- Shutdown and Isolate Systems Procedure helps asset owners make decisions about protecting other systems that may be at risk from the same cybersecurity malware infections on their network
- Problem Resolution Procedure helps asset owners identify the data they want onsite staff to collect before calling support staff so support can expedite problem resolution efforts
- 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 as their information is available.

ICS4ICS STATS

1,440 ICS4ICS members

977 companies are represented by the 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

11 ICS4ICS events (presentation, exercises) were hosted so far this year

IN THE NEWS

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

NATO Support and Procurement Agency's "Cybersecurity for Critical Infrastructure Supporting Logistics"

Megan Samford and Brian Peterson presented ICS4ICS History, Overview, and Integration with Cyber Incident Response at the NATO Support and Procurement Agency's "Cybersecurity for Critical Infrastructure Supporting Logistics" event was hosted in February!

Vytautas Butrimas and Matjaz Demsar represented ISA and presented ICS4ICS at the NATO Support and Procurement Agency's "Cybersecurity for Critical Infrastructure Supporting Logistics" event hosted in February 2024 prior to Megan Samford and Brian Peterson presenting more details about ICS4ICS.

🤝 The event was co-organized with the Office of the Under Secretary of Defense for Acquisition & Sustainment Cyber Warfare Directorate, the National Security Agency, the United States Department of Defense CIO and military departments
👥 it welcomed over 120 participants from 18 of 31 #NATO Member Nations and Sweden
💻 it focused on #cyber threats, standards, best practices, and methodologies for cybersecurity of Operational Technologies (OT) supporting critical infrastructure.

DHS JCDC Publishes "Water and Wastewater Sector - Incident Response Guide"

Megan Samford and Brian Peterson worked with DHS JCDC to develop an Incident Response Guide for the Water and Wastewater Sector:

Please find the link here (a link to a PDF is at the bottom of the page): Water and Wastewater Sector - Incident Response Guide | CISA

If anyone needs just a direct link to the PDF, you can find it here: https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf

CRESTCon 2023

CRESTCon 2023 presentation discussed ICS4ICS. Below are the links to Videos and Blogs which references ICS4ICS:

Bridging the divide between IT and OT – Presented at CRESTCon Australia 2023 | Peloton Cyber Security

Bridging the divide between IT and OT: Scott McKean & Sanam Makadia | CRESTCon Australia 2023 - YouTube

REPEAT NEWS from Last newsletter

SEC Reporting Requirements

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

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

FEMA and CISA Release Joint Guidance on Planning Considerations for Cyber Incidents

11/07/2023 01:00 PM EST

Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) released the joint guide Planning Considerations for Cyber Incidents: Guidance for Emergency Managers to provide state, local, tribal, and territorial (SLTT) emergency managers with foundational knowledge of cyber incidents to increase cyber preparedness efforts in their jurisdictions.
Emergency managers should be able to understand and prepare for the potential impacts of cyber incidents on their communities and emergency operations. FEMA and CISA encourage emergency managers to review this guide for recommendations on how to plan for and respond to cyber incidents.