



# Supplier Sharing Call

April 17, 2024

**Open Distribution for Supply Chain Materials**

Copyright © 2024 North American Transmission Forum ("NATF"). All rights reserved. Presentations are provided with the presenters' permission for distribution. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for infringement by any presentation materials, artwork, or photographs used in presentations not developed by NATF.

# NATF Members Guidelines for this Call

- This is an open call
- Some participants on this call are not employees of NATF member companies
  - Do not share confidential information
  - Avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct
  - Do not share intellectual property unless authorized

# Guidelines for this Call

- This call is not recorded
- Slides for the call will be available on the NATF public website at: [Supplier Sharing Calls \(natf.net\)](http://natf.net)

*NATF does not endorse specific solution providers and provides the webinar content for entity awareness of available resources.*

# Please Participate

- Raise your hand
  - We will unmute you
  - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

*If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request*



Tom Galloway

NATF President and CEO

# Opening Remarks

Tom Galloway,  
NATF President and CEO

# Purpose of the NATF Supplier Sharing Activities

- Provide an opportunity for suppliers to talk about cyber security issues and practices ranging from
  - How establish a security program to
  - In-depth discussions on a specific technical challenge
- Leverage knowledge from lessons learned
- Share information
- Calls will be limited to suppliers unless otherwise noted

# Contributing Organizations

- Aspen Technology / OSI
- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Laboratories (SEL)
- Siemens
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - LG&E and KU Energy
  - Nebraska Public Power District
  - Southern Company

# On this call

- Aspen Technology / OSI – Peter Escobar, VP, Research and Development
- International Society of Automation (ISA) – Andre Ristaino, Managing Director, Global Consortia and Conformity Assessment Programs
- Brian Peterson, ISA Program Manager, ICS4ICS (Incident Command System for Industrial Control Systems)
- LG&E and KU Energy – Tony Hall, Manager, CIP and Federal Regulatory Compliance
- National Electrical Manufacturers Association (NEMA) - Steve Griffith, Executive Director
- Nebraska Public Power District - Tony Eddleman, Director of NERC Reliability Compliance
- Schneider Electric – Michael Pyle, Director of Product Cyber Security
- Schweitzer Engineering Laboratories (SEL) – Frank Harrill, VP Security
- Siemens Industry – Andy Turke, Cyber Security Officer
- Siemens Energy – Christopher Fitzhugh, Industrial Control Systems Security Consultant, North America
- Southern Company – Jennifer Couch, Manager, Transmission EMS Compliance
- US Chamber of Commerce – Heath Knakmuhs, VP and Policy Counsel



# Agenda and Today's Presenters

## ICS4ICS Incident Command System for Industrial Control Systems

- **Brian Peterson**, ICS4ICS Program Manager, International Society of Automation (ISA)

## Impacts of Geopolitical Actions on Supplier Operations

*Panel discussion featuring:*

- **Christopher Fitzhugh**, Industrial Control Systems Security Consultant, North America, Siemens Energy
- **Frank Harrill**, VP Security, Schweitzer Engineering Laboratories (SEL)
- **Heath Knakmuhs**, VP and Policy Counsel, US Chamber of Commerce
- **Michael Pyle**, Director of Product Cyber Security, Schneider Electric
- **Peter Escobar**, VP, Product Security, Aspen Technology / OSI
- **Steve Griffith**, Executive Director, National Electrical Manufacturers Association (NEMA)
- *With perspectives from end-users provided by:*
  - **Tony Eddleman**, Director of NERC Reliability Compliance, Nebraska Public Power District
  - **Tony Hall**, Manager, CIP and Federal Regulatory Compliance, LG&E and KU Energy

# ICS4ICS

Incident Command System  
for Industrial Control Systems



## ICS4ICS: Program Overview and Next Steps

**NATF – North America Transmission  
Forum**

Brian Peterson  
ICS4ICS Program Manager

*April 17, 2024*



# Two years ago, we created ICS4ICS...

## The beginning of ICS4ICS

- We didn't have a common response framework, which made scaling nearly impossible
- We were bearing excessive costs due to poorly coordinated responses
- Cyber was the only designated federal disaster type not using Incident Command System for its response framework
- There was a need for consistent Cyber Incident Responder roles and typing based on experience

**It was enough to give the effort momentum, volunteers, and sponsorship through the ISAGCA (International Society of Automation Global Cybersecurity Alliance)**

# ICS4ICS Today

- Over 1,400 global volunteers and interested parties
- Completed first round of credentialing of Cyber Incident Commanders as the Adjudication Committee
  - Mark Bristow, MITRE
  - Neal Gay, Mandiant
  - Brian Wisniewski, NASA, US Army Cyber Command
  - Megan Samford, ISAGCA, Schneider Electric
- 30 additional people obtain ICS4ICS credentials
- ICS4ICS Exercises V2 were conducted in 10 locations around the world
- Utilizing FEMA materials to build ICS4ICS (thank you!)
- Oh, and its FREE – really, we're not selling anything

**ICS4ICS**  
Incident Command System  
for Industrial Control Systems



# ICS4ICS Global Reach

1,400 people in 90+ countries and 31 languages

- ICS4ICS Americas
  - 75 people in Canada
  - 125 people in Latin-America
  - 525 people in USA
- ICS4ICS Europe
  - 275 people in Europe
- ICS4ICS Middle East and Africa
  - 40 people in Africa
  - 90 people in Middle East
- ICS4ICS Asia-Australia
  - 75 people in Australia
  - 200 people in Asia

# ICS4ICS Global Reach

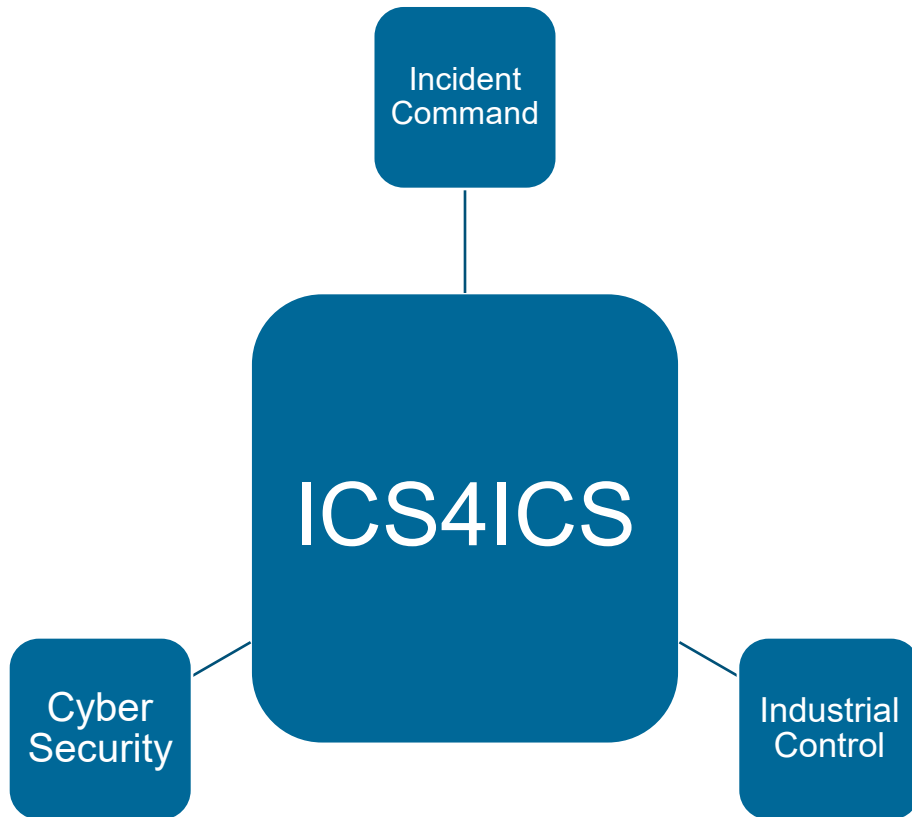
## Meeting to engage participation from volunteers

- ICS4ICS Americas-Europe-Middle East Africa monthly meetings
  - Awareness & Outreach Team schedule outreach events including exercises
  - Exercise Team is finalizing Version 2 of the exercise program
  - Training & Credentials is creating training and managing credentialling processes
  - Status meeting allow feedback from larger group of volunteers
- ICS4ICS Asia-Australia monthly meeting
  - ICS4ICS volunteers help shape the ICS4ICS program and arrange outreach events and exercises in their region
    - Status meetings allow feedback from larger group of volunteers

# ICS4ICS Overview

# ICS4ICS Improves response to cyber industrial incidents

By leveraging 3 disciplines with proven capabilities



- Incident Command System
  - Command structure to manage incidents used since the 1970's
- Cyber Security: Computer Incident Response
  - Investigation capabilities to manage cybersecurity incidents that are widely used by IT organizations
- Industrial Control System
  - Experts with Industrial knowledge and expertise to respond to incidents



# **Why use Incident Command System when managing Industrial Control System incidents?**

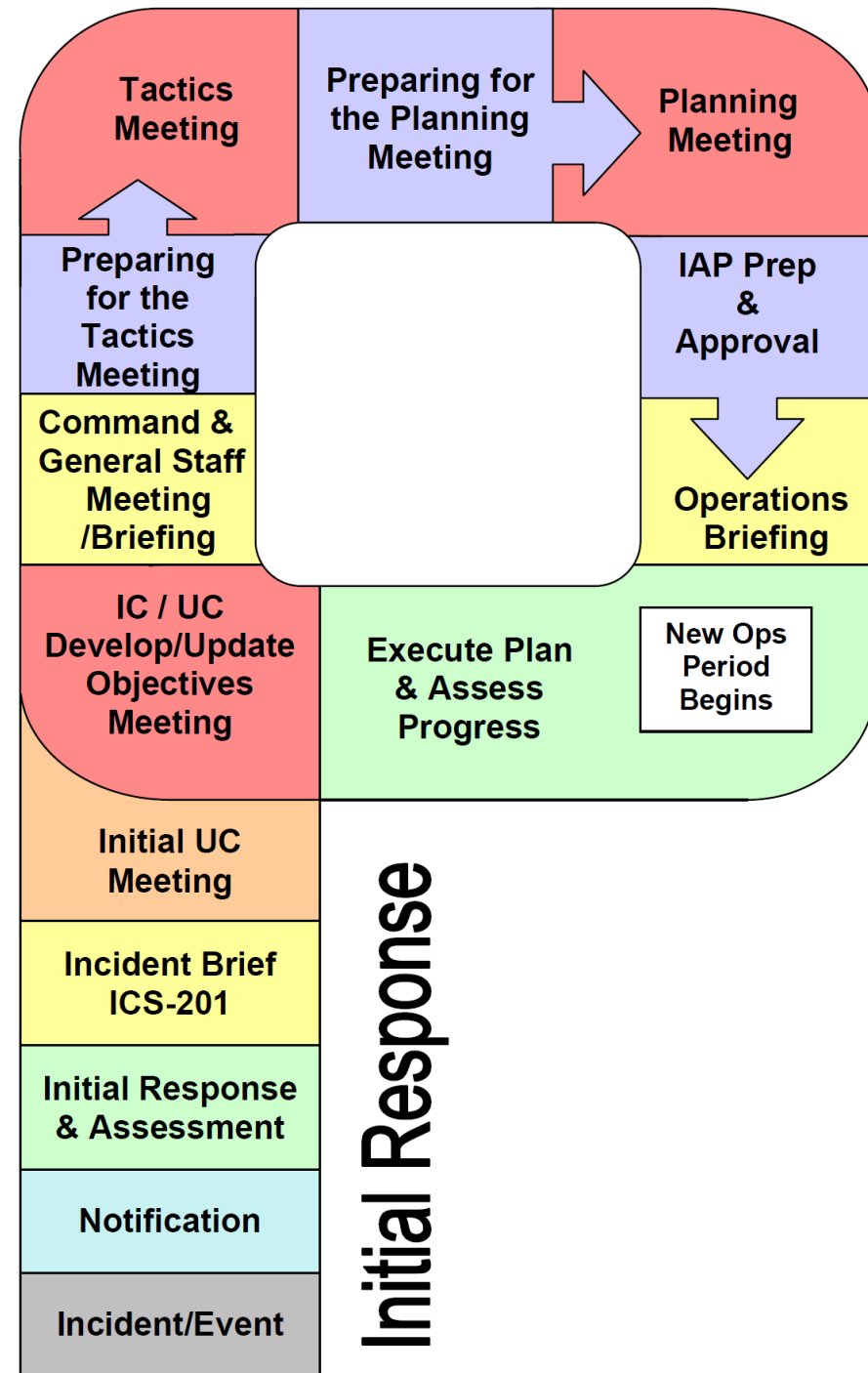
- **Standard Approach**
- **Proven Effective**
- **Unity of Command**
- **Clarity of Responsibilities**
- **Span of Control**
- **Common Terminology**
- **Adaptability to size/complexity**
- **Planned and Unplanned events**
- **Unity of Effort**
- **Accountability**

# Planning P

## Incident Command Process

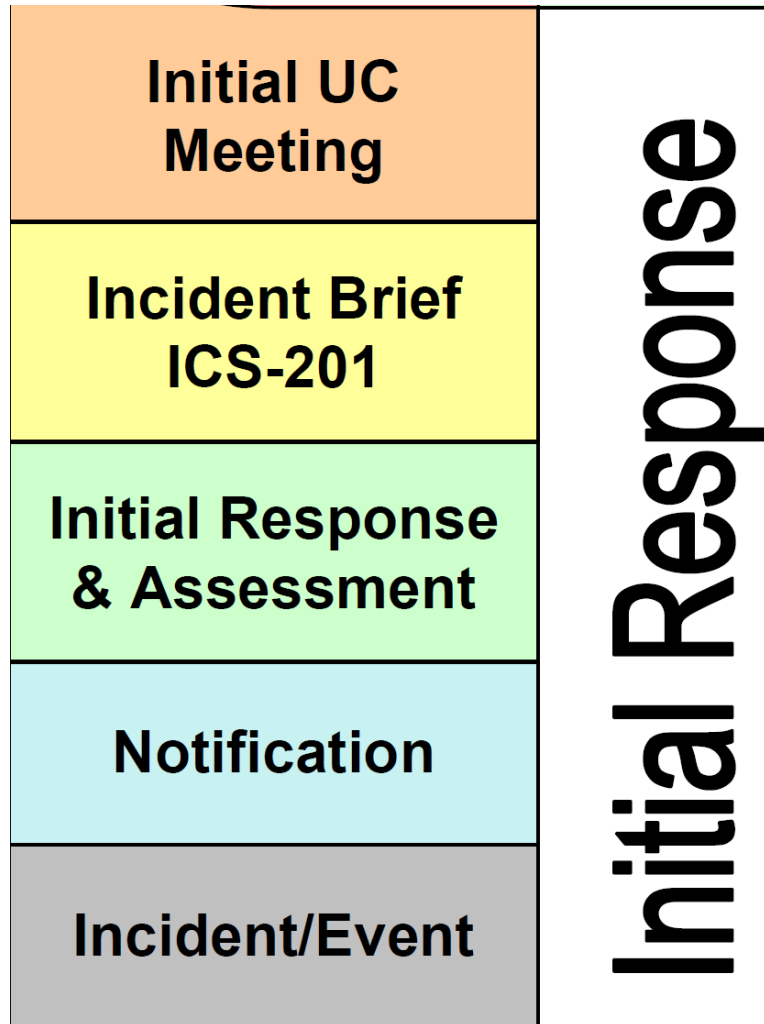
The Planning Cycle provides a proven structured process to manage any incident with a standardized approach to organizing and executing work

- Order of meetings & briefings
- Incident Command System forms & worksheets to complete
- Team member's action and/or work products



# Planning P

## Initiating Incident Response



Initial Response is the activity of evaluating an event to determine if an incident should be declared

The Incident Commander must be empowered with the authority to declare an incident, typically by senior management who are part of the Crisis Management Team

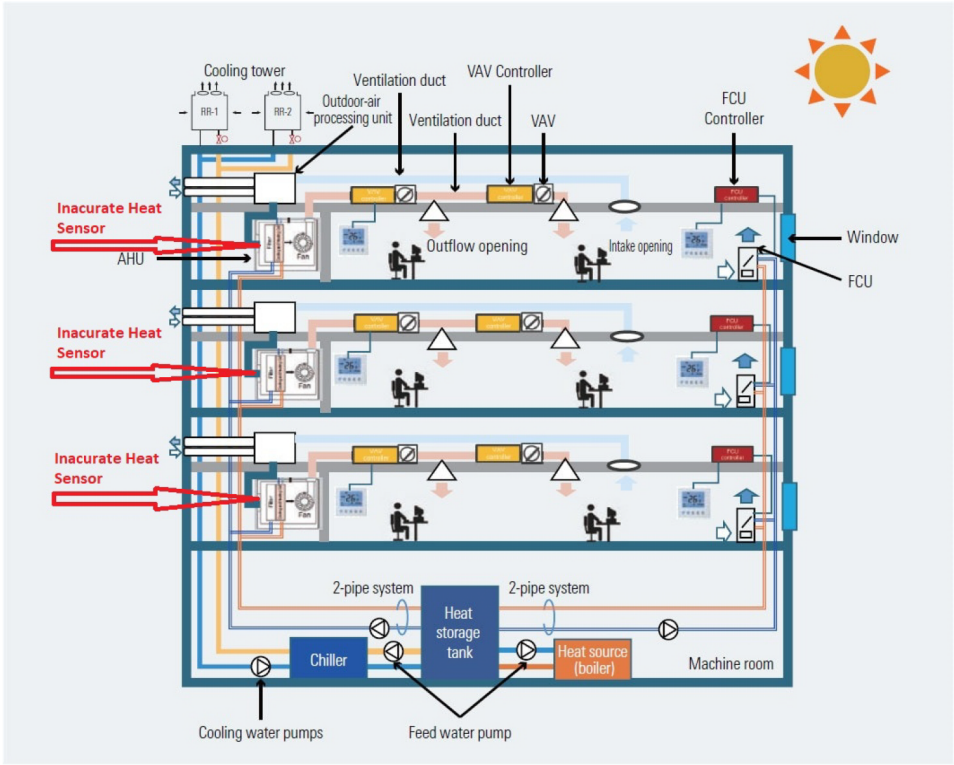
# Planning P

## Repeating the Planning Cycle

- The Planning Cycle is repeated multiple times to continue planning and working on response
  - Likely this will be repeated on a 12-hour cycle
  - The next shift will also repeat the same cycle
- The ICS4ICS Team will have to be relieved by a 2<sup>nd</sup> shift ICS4ICS Team



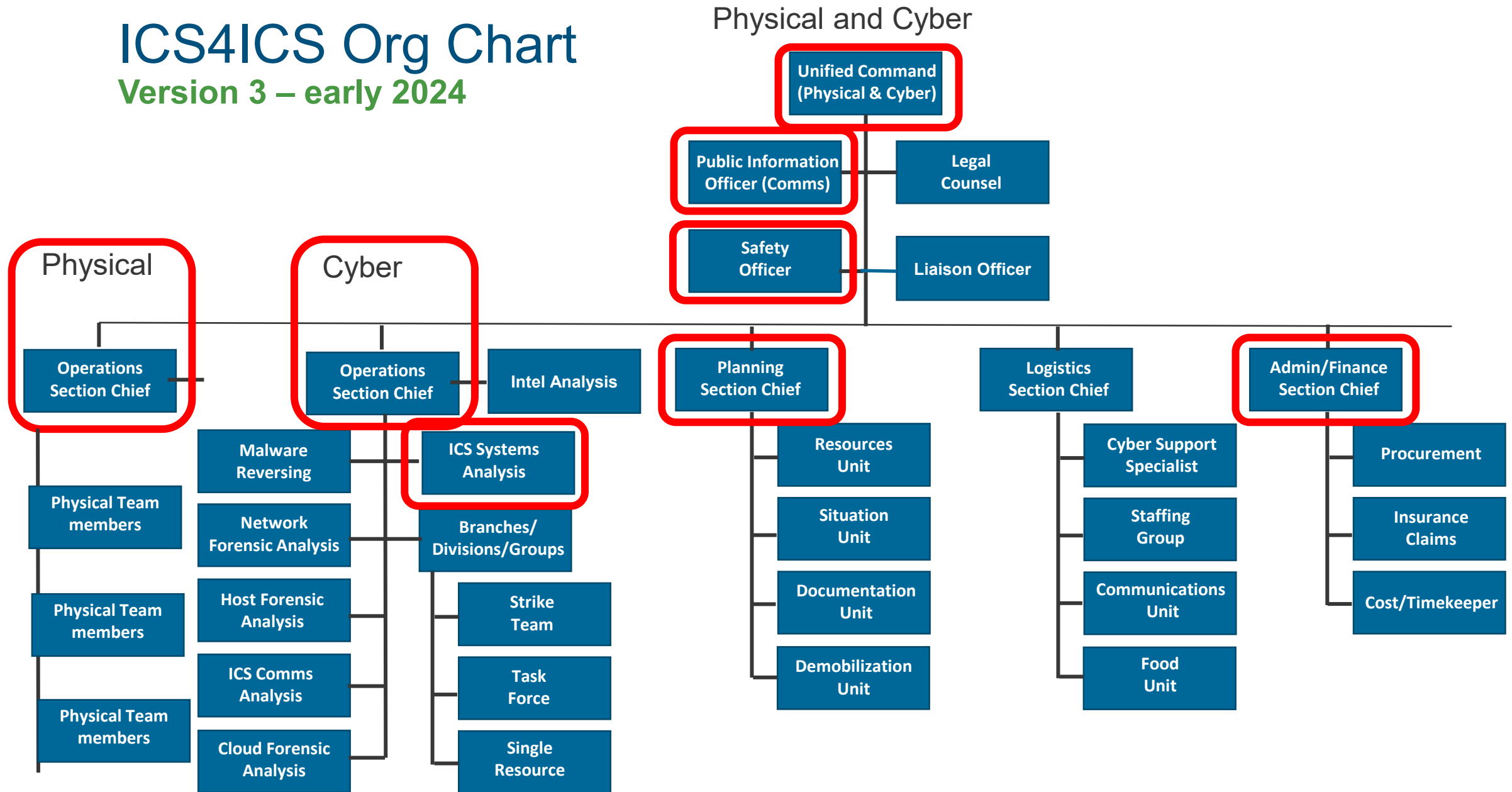
INCIDENT BRIEFING (ICS 201)

<b>1. Incident Name:</b> ICS4ICS WORKSHOP	<b>2. Incident Number:</b> N/A	<b>3. Date/Time Initiated:</b> Date: 01/24/2022    Time: 2:30 PM
<b>4. Map/Sketch</b> (include sketch, showing the total area of operations, the incident site/area, impacted and threatened areas, overflight results, trajectories, impacted shorelines, or other graphics depicting situational status and resource assignment): 		
<b>5. Situation Summary and Health and Safety Briefing</b> (for briefings or transfer of command): Recognize potential incident Health and Safety Hazards and develop necessary measures (remove hazard, provide personal protective equipment, warn people of the hazard) to protect responders from those hazards. <p>As of 1/23/2022, 9:35 hrs am, the temperature in the offices began to rise. Building Maintenance were unable to resolve the situation and HVAC Vendor was contacted.</p> <p>HVAC personnel arrived on 1/24/2022 at 10:00 am and determined that the HVAC systems has been compromised with malware. The vendor has not been able to contain or eradicate the malware and has no solutions to restored the HVAC system.</p> <p>At 10:15 am, ICS Analyst - HVAC Technical Analyst Coordinator contacts the Computer Incident Response Team (CIRT) to report that malware has been detected in the HVAC systems supporting the building, the data center, and other Industrial Control Systems in the building.</p> <p>Based on the escalation procedures, CIRT Manager declares an incident and initiates ICS4ICS.</p>		
<b>6. Prepared by:</b> Name: I. M. Scribe    Position/Title: Documentation Unit Lead    Signature: <i>I.M. Scribe</i>		
<b>ICS 201, Page 1</b>		Date/Time: 1/24/2022 3:00 pm

Incident Description

# ICS4ICS Org Chart

Version 3 – early 2024



# ICS4ICS EXERCISES

# ICS4ICS: Exercise Purpose, Mission, Objectives

**Purpose:** To explain proposed approach to coordination, collaboration, information sharing, and response capabilities of ICS4ICS in the context of a significant cyber incident that might result in physical threats to life, safety, and property.

**Mission:** Highlight the approach that ICS4ICS is recommending to manage a Cyber Security Incident for Industrial Control System

## Objectives

1. Monitor events to identify possible incidents
2. Perform Notification to engage ICS4ICS Team
3. Complete an initial Assessment of the event and declare Incident if appropriate
4. Bring ICS4ICS program capabilities into organizations' existing Incident Response program
5. Stand-up an ICS4ICS structure and exercise key components of the program
6. Work on Remediation and Resolution of incident

**Threat/Hazard:** Cyber Security Incident impacting Industrial Control System, HVAC



# ICS4ICS: Exercise are Different

More of a demonstration to help people learn

- **ICS4ICS Exercises are fully scripted**
  - Enables participants to learn the Incident Command System
  - Players can have limited knowledge of NIMS/ICS or ICS4ICS
- **ICS4ICS Exercises in various duration and formats**
  - 1-hour video prepares players for the ICS4ICS Exercise
  - 2-hour, 3-hour, and all-day ICS4ICS Exercise are available
  - Hybrid exercise mixes short video segments with participant participation
- **ICS4ICS Exercises**
  - 12 ICS4ICS Exercises were conducted in various countries
  - Chemical company conducted an all-day ICS4ICS Exercise that verified materials
  - Industry specific exercises were hosted, and more are planned in 2024

# ICS4ICS: Exercises require participants engagement

## Building the ICS4ICS program through exercise player/participant feedback

- ICS4ICS Exercise materials have been updated based on player/participant feedback
  - Exercise materials continue to be updated to reduce redundancy, create more exercise player interaction, and demonstrate evolving incidents and actions
- ICS4ICS procedures, tools, and templates were developed/reviewed during exercises
  - Most of the ICS4ICS resources were written during an ICS4ICS exercise
    - Ransomware, Gov Reporting, IT procedures, Cyber Insurance, etc.
- ICS4ICS Program goals and strategies are based on feedback
  - For example, focus on small companies (water), priority of ICS4ICS work, etc.

# ICS4ICS: After Action notable feedback – So Far...

## Hot Wash Remarks/Comments

- ICS4ICS processes, forms and other resources can be used for big or small incidents
  - The size of the ICS4ICS team will vary greatly based on the incident!
- Small companies need help to use ICS4ICS
  - We are focused on water utilities
- Delegation of Authority (DOA) is critical to declare and finance an incident
  - DOA procedure has been drafted
- Tighter integration is needed between NIMS/ICS and OT/IT Staff
  - More resources needed to help these parties work together
- OT/IT Procedures are needed to ensure that timeline response
  - OT and IT Technical procedures are needed to quickly make decisions and act
- Procedures and processes are very valuable
  - Ransomware, DOA, Escalation-Declaration-Notification, External Info Resources, Gov Reporting, BCP/IT DR, etc.

# ICS4ICS Resource: Required for Pre-Requisites

## Ensuring Asset Owners have foundational processes

- ICS4ICS is creating additional resources to ensure that Asset Owners have created foundational processes required to manage an incident
  - Delegation of Authority must be established before an incident to:
    - Enable the Incident Commander to declare an Incident
    - Enable various ICS4ICS team members to have sufficient financial authorities
  - IT/OT Recovery and BCP processes must be understood as an option to restore critical business operations AND to support the ICS4ICS Team
  - Government Reporting requirements and processes
  - External informational resources (e.g., DHS CISA, various gov)

# Training & Credentials

# ICS4ICS: Credentials

## Providing consistent organizational capabilities to execute ICS4ICS

- ICS4ICS Exercise are used to prepare players for ICS4ICS Credentials
- ICS4ICS Type 4 Credentials enable people to perform roles for simple incidents:
  - Incident Commander
  - Operations, Planning, Logistics, and Admin/Finance Section Chiefs
  - Public Information Officer (PIO) and Safety Officer
- ICS4ICS leverages FEMA training for obtaining credentials
  - 15 to 20 hours of training is required depending on the role
- We will add other key ICS4ICS roles
  - Document Unit Leader, Liaison Officers, and other roles
- Partnering with INL to complete skill profiles for technical roles
  - For example, Forensics, Malware, and various OT and IT roles

# ICS4ICS: Training Available Today

## Sharing knowledge about ICS4ICS

- ICS4ICS leverage FEMA provided training
- ICS4ICS-specific Training materials consist of videos on YouTube
  - 2-hour ICS4ICS Overview Training course help people understand the program
  - Two short Planning-P training modules explain NIMS/ICS
  - A short video explains the various ICS4ICS meetings
  - 1-hour Exercise video helps people understand how an ICS4ICS Team works together to manage an incident enable faster resolution and allowing the Cyber Incident Response to do their jobs

# ICS4ICS 2024 Program Plan



# ICS4ICS: 2024 Program Plan – Training & Credentials

## Sharing knowledge and learning about ICS4ICS

- ICS4ICS Training materials and courses are being developed in 2024
  - Partner with INL on Work Force Development (WFD) Skills Assessment to identify ICS4ICS skills and tools to assess organizational skill gaps
  - 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
  - Update Role Sheets for critical roles including liaison officers, safety roles, and others
  - Partner with other training efforts (e.g., DOE CYMANII, INL ICS-301) to include ICS4ICS training in their programs
  - Continue to expand the ICS4ICS Credentialling program with more roles and Type 3

# ICS4ICS: 2024 Program Plan – Awareness & Outreach

## Sharing knowledge and learning about ICS4ICS

- Finalize updates to the new ICS4ICS website
- Create ICS4ICS Overview whitepapers and video to help show how various aspects of the program work together
- Document how to create joint Cybersecurity Incident Response and ICS4ICS exercises and describe how these processes align
- Develop marketing materials that describe the value of ICS4ICS
  - Used to engage management, gov, others to seek their support for ICS4ICS
  - Senior leaders from an Asset Owner must support ICS4ICS company-wide
    - Company policies must be updated to ensure ICS4ICS is adopted by all teams
- Engage globally to reference ICS4ICS from their website, etc. (e.g., Charter of Trust-like)
  - Government agencies, ISACs, Associations, etc. AND ask their members to join
- Continue to identify and manage ICS4ICS Awareness & Outreach exercises, presentations, and other opportunities - These efforts are primarily driven by ICS4ICS member volunteers

# ICS4ICS 2024 Program Plan - Exercises

## Expanding knowledge through exercises and resources

- ICS4ICS Version 3 will be created in (early) 2024 to include exercise for:
  - Unified Command (UC) with a simulation of a physical incident (e.g., fire) caused by a cyber incident
  - Expand exercises to include Type 3 incidents which are a Single Company with Multiple Sites impacted
  - Cybersecurity Incident Response and ICS4ICS joint exercises – Consider adding AI role
  - Industry specific ICS4ICS exercises (water, electric, etc.) – we are seeking more industries
- ICS4ICS Resources will be added
  - Publish ICS4ICS Resources (procedures, templates, tools) 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, Cybersecurity, and other processes
  - Add resources based on feedback from the ICS4ICS members and Exercise Hot-Washes

# Getting Involved in ICS4ICS

# ICS4ICS and you

## How can you get involved?

- Visit or website: [www.ics4ics.org](http://www.ics4ics.org)
- Register for the ICS4ICS Newsletter
- Observe or Participate in an ICS4ICS exercise
- Host an ICS4ICS exercise at a public event or in your company
- Join an ICS4ICS team to help define the processes, training, etc.
- Consider presenting ICS4ICS at a future event

**Contact Brian Peterson [bpeterson@isa.org](mailto:bpeterson@isa.org) for more information**

**Q&A**

# ICS4ICS Resources

- ICS4ICS's First Virtual Exercise: [ICS4ICS Virtual Exercise V3-20240411.mp4 \(sharepoint.com\)](#)
- ICS4ICS website: <https://www.ics4ics.org/>

# The Impact of Geopolitical Actions on Suppliers' Operations

*Panel Discussion Featuring:*

**Christopher  
Fitzhugh**

Industrial Control  
Systems Security  
Consultant, North  
America, Siemens  
Energy

**Frank Harrill**

VP Security,  
Schweitzer  
Engineering  
Laboratories (SEL)

**Heath  
Knakmuhs**

VP and Policy  
Counsel, US  
Chamber of  
Commerce

**Michael Pyle**

Director of Product  
Cyber Security,  
Schneider Electric

**Peter Escobar**

VP, Product Security,  
Aspen Technology /  
OSI

**Steve Griffith**

Executive Director,  
National Electrical  
Manufacturers  
Association (NEMA)

**With:**

**Tony Eddleman**, Director of NERC Reliability Compliance, Nebraska Public Power District  
and

**Tony Hall**, Manager, CIP and Federal Regulatory Compliance, LG&E and KU Energy



# Discussions

- Recent Incidents and Threats
- Government and Sentiment Influence
- Supplier Impacts and Mitigation
- Sourcing

# Recent Incidents and Threats

*Discussion Lead: Frank Harrill*

## Discussion Points:

- Degree of intelligence available for current incidents
- Little or no utilization of AI tools
- Many of these are largely preventable

# Recent Incidents and Threats

*Discussion Lead: Frank Harrill*

## Links provided during webinar:

- Joint guidance - Identifying and Mitigating Living Off the Land intrusions: <https://media.defense.gov/2024/Feb/07/2003389936/-1/-1/0/JOINT-GUIDANCE-IDENTIFYING-AND-MITIGATING-LOTL.PDF>
- Defense industrial base cybersecurity services: <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>
- Staying ahead of threat actors in the age of AI: <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>
- Cyber Safety Review Board report: [https://www.cisa.gov/sites/default/files/2024-04/CSRB\\_Review\\_of\\_the\\_Summer\\_2023\\_MEO\\_Intrusion\\_Final\\_508c.pdf](https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf)
- XZ Utils supply chain compromise: <https://research.swtch.com/xz-timeline>
- Open JS foundation attempt: <https://therecord.media/researchers-stop-credible-takeover-xz-utils>

# Government and Sentiment Influence

*Discussion Leads: Heath Knakmuhs, Christopher Fitzhugh, and Michael Pyle*

## Discussion Points:

- Pervasive agreement in Washington DC and specifically Congress
- International suppliers looking for international standards and acceptance
- Need for international requirements or regulation
- Sentiment impacting acceptance and supplier sales (e.g., cranes from China)

# Supplier Impacts and Mitigations

*Discussion Lead: Steve Griffith*

## Discussion Points:

- Manufacturers manage dependencies with tier 1 and sub-tier (2-x) suppliers
  - Assess, mitigate, respond, and remediate
  - Continuous monitoring and vulnerability response programs
- Impacts when manufacturers can't, or shouldn't, get parts from their suppliers
  - Impacts on costs by keeping extra inventory
  - Impacts on delivery dates
  - Differences for small and medium sized companies

# Sourcing

*Discussion Lead: Michael Pyle*

## Discussion Points:

- Source in the United States
- Considerations for sourcing decisions for software and component parts (e.g., semi-conductors).
  - Regulation comes into play – consider what parts may be banned in different countries and export laws



Questions?

Comments?

# Upcoming Calls

- June 19 – Discussion on Software Bills of Materials (SBOMs)
- Special Webinar – May 29

*NATF and ISA Special Webinar: The NATF Criteria and Questionnaire Update:  
Mapping to Certifications*





Frank Harrill

VP, Security, SEL

# Closing Remarks

Frank Harrill  
VP, Security Schweitzer Engineering (SEL)

# Thank you for attending!

[supplychain@natf.net](mailto:supplychain@natf.net)

[dearley@natf.net](mailto:dearley@natf.net)

[vagnew@natf.net](mailto:vagnew@natf.net)