ICS4ICS-Incident Command System for Industrial Control Systems

Megan Samford, Chair, ISA Global Cybersecurity Alliance

Andre Ristaino, ISA

Sharing more information about ICS4ICS

Aug 2021

ISA Global Cybersecurity Alliance

Bridge the gap between publication of the 62443 standards and adoption by stakeholders.

- Awareness & Outreach
- Advocacy & Adoption
- Compliance & Prevention
- Training & Education

- Launched July 2019
- 50 members currently
- Added industry groups – LOGIIC, ISASecure, ISA99; in discussion with others
- Globalize - Establish regional teams for outreach activities and regulatory tracking (NA, EU, Japan, MEA) in 2020
- Complete 8 key projects in 2020

What is ICS4ICS?

Public / private partnership based on the FEMA Incident Command System that provides for:

- Standard response plan templates
- Standard terminology
- Role descriptions (resource typing)
- Mutual aid/surge capacity
- Standard After-Action Reports (AARs)/Improvement Plans and tabletop exercises
- Tie into Continuity of Operations Plans (COOP)

Similar to electric power company resource sharing for responding to natural disasters that damage power generation and distribution infrastructure serving their customers.

Benefits of ICS4ICS

- Provides a means for the private sector to organize into a common framework to support basic company to company mutual aid in the event of a large-scale cyber incident.
- ICS4ICS addresses the challenges stemming from the fact that private-sector cybersecurity is a ‘distributed’ problem that must be addressed locally from the bottom-up.
- Multiplies response and rebuild capabilities for private sector companies.
- Amplifies public-sector resources, capabilities and, leadership
- ICS4ICS will establish a self-sustaining long-term cybersecurity response capability that transcends individual companies and people over time.

ICS Org Snapshot

COMMAND

- Defines the incident goals and operational period objectives. Operational periods typically run for 6, 8, or 12 hours
- Includes an Incident Commander, or Unified Command when two sides share equal responsibility, Safety Officer, Public Information Officer, Legal and other senior advisors

OPERATIONS

- Establishes strategy (approach methodology, etc.) and specific tactics (actions) to accomplish the goals and objectives set by Command
- Coordinates and executes strategy and tactics to achieve response objectives

PLANNING

- Coordinates support activities for incident planning as well as contingency, long-range, and demobilization planning
- Supports Command and Operations in processing incident information
- Coordinates information activities across the response system

LOGISTICS

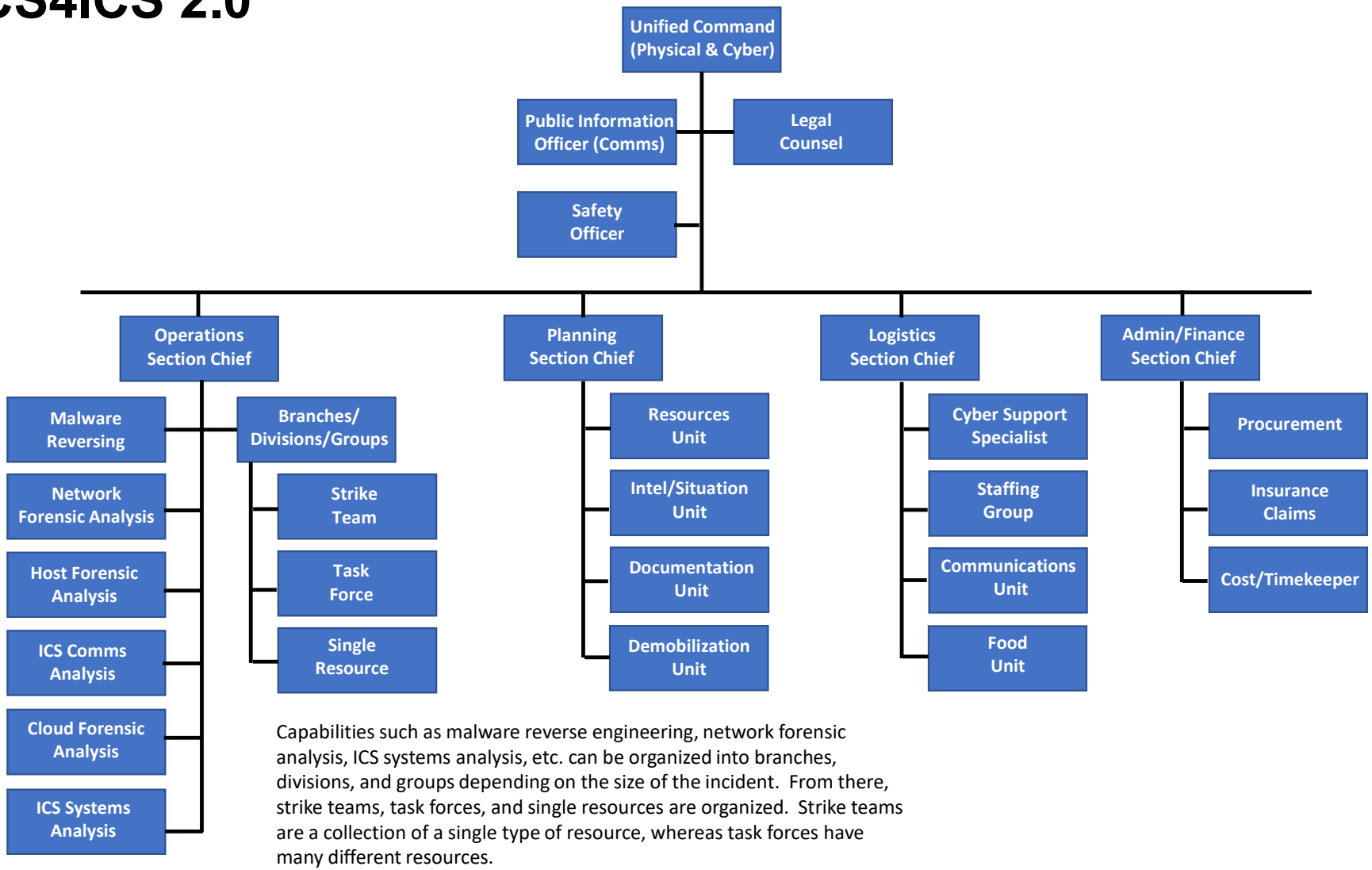
- Supports Command and Operations in their use of personnel, supplies, and equipment
- Performs technical activities required to maintain the function of operational facilities and processes

ADMIN/FINANCE

- Supports Command and Operations with administrative issues as well as tracking and processing incident expenses
- Includes such issues as licensure requirements, regulatory compliance, and financial accounting

Source: U.S. Dept of Health & Human Services

ICS4ICS 2.0



Capabilities such as malware reverse engineering, network forensic analysis, ICS systems analysis, etc. can be organized into branches, divisions, and groups depending on the size of the incident. From there, strike teams, task forces, and single resources are organized. Strike teams are a collection of a single type of resource, whereas task forces have many different resources.

ICS4ICS Project Plan

Task	3Q21	4Q21	1Q22
Establish ICS4ICS Advisory Team	X		
Approve ICS4ICS Project Charter	X		
Identify ICS4ICS Project Team members, reviewers, etc.	X		
Create ICS4ICS Website with initial content	X		
Develop ICS4ICS funding alternatives and seek funds	X		
Document ICS4ICS procedures, processes, and tools	X	X	
Establish ICS4ICS training program and education providers		X	X
Define the ICS4ICS certification requirements for various roles		X	X
Create and schedule ICS4ICS exercises		X	X
Transition ICS4ICS to owning organization			X

ICS4ICS Project Volunteers NEEDED

- Tasks to perform
  - Author ICS4ICS materials, articles, etc.
  - Share existing materials and resources that can be leveraged publicly
  - Review ICS4ICS materials and provide feedback
- Experiences Needed
  - Incident command or response experience (general or cybersecurity)
  - Training & Education for incident command or response
  - Incident command or response program develop or management
  - Exercising Incident command or response
- Time commitment
  - Varies based on availability

Q&A

Enabling Response Capabilities

Requires ‘prepositioning’ resources, ready to respond on short notice:

- Pre-defined organization including leadership structure
- Communication, command and control
- Legal agreements for resource sharing
- Availability of technical personnel, technology and, tools
- Readiness exercises
- Rotation of leadership responsibilities and succession plans

Roles of Collaborators

- ISAGCA – Provides the forum for organizing and standing-up the ICS4ICS. Also provides a resource pool for, recruiting for and, augmenting ICS4ICS personnel capabilities.
- Asset Owners and End-users- Prime beneficiaries of the shared resources. They contribute personnel, tools and, capabilities on a shared basis when needed.
- FEMA-Provides collaboration applications, templates for resource sharing agreements, operational models, advice on organizing.
- DHS and INL-provide conduit to government resources for organizing the ICS4ICS and when resources are needed during an incident.