

Mutual Aid

ICS4ICS Procedure Template

|  |
| --- |
| Instructions The following are suggestions about how you can update this template to create a procedure for your company:   * Identify the roles required on the Decision Team that will manage Mutual Aid decisions * Review and update the Decision Considerations based on your company requirements * Test this Mutual Aid Procedure and update as appropriate |
| DisclaimerISA, ISAGCA, and the ICS4ICS Program provide this template to help asset owners create procedures to perform ICS4ICS and/or Cyber Incident Response and/or other related tasks. Each Asset Owners must update this template based on the needs of their company and ensure the procedure is review and approved by the appropriate parties (e.g., legal, senior management, corporate governance, government relations, etc.) from within their company. |

# Purpose

This document is intended to provide information to describe how <<company>> will leverage mutual aid that may be required to staff some positions in the Cyber Incident Response and ICS4ICS teams.

# Situation Trigger

An incident has been declared by the ICS4ICS Incident Commander and the Operations Section Chief and others in the ICS4ICS organization have identified they need additional staff.

# Mutual Aid General Information

Mutual aid is often critical to allow an asset owner to assemble an ICS4ICS team with critical roles being staffed particularly during extreme incidents. Asset owners may not have internal staff to perform some of the technical roles required on the ICS4ICS team. Some of the roles that may need to be staffed through a mutual aid agreement include Forensics Analyst, Malware Reverse Engineer, Intelligence Analyst, and other roles.

Mutual aid agreements establish the terms under which one party provides resources—personnel,

teams, facilities, equipment, and supplies—to another party. Mutual aid agreements provide a means for asset owners to augment their staffing resources when needed for high demand incidents. Mutual aid agreements between private companies establish how asset owners engage and pay for services from other parties. These other parties may include service companies, other asset owners, and other parties who can staff ICS4ICS roles.

The mutual aid processes for asset owners have some similarities to how government entities provide mutual aid but there are some significant differences. Government entities may provide mutual aid to each other with limited consideration of funding. Asset Owners are commercial companies who must pay for mutual aid services regardless of who provides them. These are the two primary types of mutual aid for Asset Owners:

* **Service Provider Mutual Aid**: Numerous Service Providers can assist with various aspects of incident management to fill roles on the ICS4ICS team. These service providers often provide technical staff who would be part of the ICS4ICS Operations Section.
* **Asset Owner Mutual Aid**: Asset Owners may decide to provide mutual aid to each other particularly when it is difficult to obtain other staff, like in remote countries in the world. Asset Owners can assist each other with various aspects of incident management to fill roles on the ICS4ICS team.

ICS4ICS Mutual Aid processes were developed based on: [National Incident Management System - Guideline for Mutual Aid (fema.gov)](https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf#:~:text=The%20National%20Incident%20Management%20System%20Guideline%20for%20Mutual,entering%20into%20a%20mutual%20aid%20agreement%20or%20compact.) from November 2017.

Mutual Aid Training is available: [FEMA - Emergency Management Institute (EMI) Course | IS-706: NIMS Intrastate Mutual Aid - An Introduction](https://training.fema.gov/is/courseoverview.aspx?code=IS-706&lang=en)

# Mutual Aid Planning

An Asset Owner must determine what type of mutual aid they need. They can complete a risk assessment to identify potential shortfalls and capability gaps that a mutual aid agreement can help to address. Before your organization decides to enter into a mutual aid agreement, be sure to:

* Identify staffing resources that your company will need during an incident
  + Define the roles your company needs to staff your ICS4ICS team based on likely incident that can impact your assets
* Inventory company personnel who can staff the needed positions
  + Identify people within your company who can fill the roles on your ICS4ICS team
* Qualify, certify, and credential personnel from your company
  + Understand the type of ICS4ICS credentials your staff have obtained
  + Also, consider the type of ICS4ICS credentials your staff have obtained (e.g., Type 4 to 1)
* Plan for staffing resources that need to be obtained through mutual aid
  + Identify the ICS4ICS roles your company cannot staff internally
  + Select a Mutual Aid service provider who can provide staff to fill the roles you are not able to fill internally

NOTE: When planning the number of resources that are needed to manage an incident you must consider that many incident teams work in 12-hour shifts so additional staff are needed for the 2nd shift. In addition to staffing for a first and second shift, alternative staff will need to be identified to fill positions if the primary staff is not available (e.g., on vacation).

# Mutual Aid Agreements

Mutual aid is only valuable if agreements can be established quickly to enable other parties to fill roles on the ICS4ICS team. The ICS4ICS Program Manager and ISA organization will not participate in establishing agreements between various parties. We recommend that Asset Owners complete Mutual Aid Planning and then an exercise to determine what ICS4ICS roles they will not be able to staff internally. Then they can identify a mutual aid partner to fill those roles.

Mutual aid agreements can vary considerably from agreement to agreement. The participating parties determine the content and structure of an agreement or compact. An Asset Owner may enter into multiple agreements with varying formats and content. Common terminology and formats and writing in plain English help clarify expectations, promote unity of effort, and expedite mutual aid efforts. When establishing mutual aid agreements or compacts, jurisdictions and organizations should address the following key elements to improve the understanding of the commitment, scope, and general procedures for all parties.

More information about Key Elements of Mutual Aid Agreement can be found at: [National Incident Management System - Guideline for Mutual Aid (fema.gov)](https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf#:~:text=The%20National%20Incident%20Management%20System%20Guideline%20for%20Mutual,entering%20into%20a%20mutual%20aid%20agreement%20or%20compact.) (November 2017). Some key elements have been summarized [Attachment #1 - Key Elements of Mutual Aid Agreements](#_Attachment_#1_-)

# Mutual Aid Operational Plans

Mutual aid operational plans support mutual aid agreements and guide the Asset Owners and Service Providers in managing and providing effective mutual aid. Though not required, these plans are essential to identify specific resources, tasks, personnel, asset allocations, roles, responsibilities, integration, and actions that mutual aid participants execute respective to their assignments. Mutual aid operational plans:

* Supplement mutual aid agreements, either as an appendix to the agreement or as a separate document
* Identify specific resources, tasks, personnel, asset allocations, roles, responsibilities, integration, and actions that mutual aid participants execute respective to their assignments; and
* Help requesting or receiving parties manage mutual aid assets during a planned event or following an incident.

The key characteristics and components of effective mutual aid operational plans have been summarized [Attachment #2 - Mutual Aid Operational Plans](#_Attachment_#2_-)

# ICS4ICS Roles

During the Mutual Aid Planning effort, a risk assessment should be completed to identify potential shortfalls and capability gaps that a mutual aid agreement can help to address. These are some of the roles that an ICS4ICS team may need to staff through mutual aid based on the type of incident:

|  |  |  |
| --- | --- | --- |
| ICS4ICS role | Description (brief) | Recommend |
| Operations Section Chief | Lead the ICS4ICS Operations Section |  |
| Intelligence Analyst | Evaluate info to identify/mitigate security threats |  |
| Malware Reverse Engineer | Deconstruct malware to identify corrective actions |  |
| ICS System Analyst | Provide expertise of specific ICS solution / business |  |
| ICS Communications Analyst | Provide ICS Communication expertise |  |
| Network Forensics Analyst | Analyze network packets to identify root causes |  |
| Host Forensics Analyst | Analyze host logs/data to identify root causes |  |
| Cloud Forensics Analyst | Analyze cloud logs/data to identify root causes |  |
| Other roles can be found at: |  |  |
|  | [NQS\_OneResponder\_Manager (fema.gov)](https://oneresponder.preptoolkit.fema.gov/manager/home/landing) |  |
|  | [Mission Ready Packages (emacweb.org)](https://www.emacweb.org/index.php/learn/mission-ready-packages) |  |
|  | [Resource Typing Library Tool - RTLT (fema.gov)](https://rtlt.preptoolkit.fema.gov/Public)  [Typing Library - RTLT (fema.gov)](https://rtlt.preptoolkit.fema.gov/Public/Combined?s=&a=&q=cybersecurity) |  |

These are roles typically staffing internally (in-house) by the company)

|  |  |  |
| --- | --- | --- |
| ICS4ICS role | Description (brief) | Recommend |
| Incident Commander | Lead the ICS4ICS Team  Report to and interface with senior executives | In-house |
| Public Information Officer | Manage communications with media, public, etc. | In-house |
| Legal Counsel | Provide legal advice about ICS4ICS decisions | In-house |
| Liaison Officer | Coordinate with other organizations on incident | In-house |
| Planning Section Chief | Lead the Planning Section  Manage planning activities for Operations Section | In-house |
| Resources Unit Leader | Maintain status of assigned resources at an incident |  |
| Situation Unit Leader | Organize, evaluate, analyze, and display incident info |  |
| Documentation Unit Leader | Maintain documentation during an incident |  |
| Logistics Section Chief | Lead the Logistics Section  Provide facilities/services/materials for incident team | In-house |
| Cyber Support Specialist | Provide IT resources needed for incident team |  |
| Admin/Finance Section Chief | Lead the Admin/Finance Team  Manage finances and admin tasks for incident team | In-house |
| Procurement Analyst | Procure resources needed to manage the incident | In-house |
| Insurance Analyst | Understand and manage insurance activities | In-house |
| Cost/Timekeeper | Establish and manage process to track costs and labor | In-house |

Note: Consider using “In-house” resources based on the “Recommend” column.

# ICS4ICS Mutual Aid Providers

This section provides a list of organizations that provide services to fill some of the ICS4ICS specific staffing roles. This section is limited to ICS4ICS cybersecurity roles. If the incident includes other aspects, Unified Command will need to find other alternatives for mutual aid for non-cybersecurity roles.

DISCLAIMER: ISA, ISAGCA, nor the ICS4ICS Program make any claims or endorsements about any specific mutual aid providers. You should perform due diligence to select the mutual aid provider who meets your incident management needs.

## Dragos

Dragos is the Industrial Cybersecurity experts on a relentless mission to safeguard civilization. We are devoted to codifying and sharing our in-depth industry knowledge of ICS/OT systems and arming industrial defenders around the world with the knowledge and tools to protect their systems.

<https://www.dragos.com/>

|  |  |  |
| --- | --- | --- |
| ICS4ICS role | Additional Information | Other |
| Intelligence Analyst | Threat intelligence team provides expert insights from threat hunting and responding to significant ICS threats. | <https://www.dragos.com/dragos-threat-intelligence/> |
| Malware Reverse Engineer | Malware analysis team provide detailed analysis of capabilities, intent, attack vector, motivation, and tactics |  |
| ICS System Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| ICS Communications Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Network Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Host Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Cloud Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |

## Resources for Building a Foundational OT Cybersecurity Program

### Dragos OT-CERT

OT-CERT is an Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gap that exists in industrial infrastructure. Designed to support asset owners and operators of industrial infrastructure, Dragos OT-CERT provides free cybersecurity resources for the Industrial Control System (ICS) /OT community.

<https://www.dragos.com/ot-cert/>

* OT-CERT provides free resources for the ICS/OT community, providing members with information and materials to help build an OT cybersecurity program, improve their security posture, and reduce OT risks.
* Collaboration allows us to leverage our combined experience and contribute to the ICS community for long-term industry impact. OT-CERT workshops conducted jointly with partners will build a trusted advisor relationship and promote information sharing among members of the partner organization.
* Membership is open to organizations globally, and firms of any size are welcome to join. Sign up to be a part of the OT-CERT community and get access to new resources monthly from the OT-CERT portal.

Dragos is the Industrial Cybersecurity experts on a relentless mission to safeguard civilization. We are devoted to codifying and sharing our in-depth industry knowledge of ICS/OT systems and arming industrial defenders around the world with the knowledge and tools to protect their systems.

<https://www.dragos.com/>

|  |  |  |
| --- | --- | --- |
| ICS4ICS role | Additional Information | Other |
| Intelligence Analyst | Threat intelligence team provides expert insights from threat hunting and responding to significant ICS threats. | <https://www.dragos.com/dragos-threat-intelligence/> |
| Malware Reverse Engineer | Malware analysis team provide detailed analysis of capabilities, intent, attack vector, motivation, and tactics |  |
| ICS System Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| ICS Communications Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Network Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Host Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |
| Cloud Forensics Analyst | Professional Services Team – Rapid Response | <https://www.dragos.com/services/> |

Note: <other notes>

## Resources for Building a Foundational OT Cybersecurity Program

### Dragos OT-CERT

OT-CERT is an Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gap that exists in industrial infrastructure. Designed to support asset owners and operators of industrial infrastructure, Dragos OT-CERT provides free cybersecurity resources for the Industrial Control System (ICS) /OT community.

<https://www.dragos.com/ot-cert/>

* OT-CERT provides free resources for the ICS/OT community, providing members with information and materials to help build an OT cybersecurity program, improve their security posture, and reduce OT risks.
* Collaboration allows us to leverage our combined experience and contribute to the ICS community for long-term industry impact. OT-CERT workshops conducted jointly with partners will build a trusted advisor relationship and promote information sharing among members of the partner organization.
* Membership is open to organizations globally, and firms of any size are welcome to join. Sign up to be a part of the OT-CERT community and get access to new resources monthly from the OT-CERT portal.

# ICS4ICS Mutual Aid - Attachments

## Attachment #1 - Key Elements of Mutual Aid Agreements

This is a summary of Key Elements of Mutual Aid Agreements which should be signed in a contract prior to an incident and then a workorder (W/O) can be created to execute the agreement when the incident occurs:

* **Purpose and Scope**: Identify the agreement’s conditions, length, and general legal scope or effect, such as the intent to bind parties or severability. Present the reason for the agreement and identify the parties, the types of services addressed, and any applicable mutual aid service limitations. Organizations often specify whether the agreement’s intent is to provide resources for declared disasters or surge capacity prior to a disaster declaration. **W/O Clarification**
* **Benefits**: Outline the economic, logistical, or other benefits that the mutual aid agreement may provide to the parties entering into the agreement.
* **Authorities**: Specifically state the legal basis for the parties to enter into the mutual aid agreement in an “authorities” section.
* **Definitions**: Define key terms in the agreement to ensure all parties share a common vocabulary, especially any terms that are specific or unique to the circumstances of the contract.
* **Governance Structure and Operations Oversight**: The governance section should specify who is responsible for overseeing the agreement and how those personnel communicate policies and procedures to guide the agreement’s implementation and operation.
* **Recognition of Licensure and Certifications**: Identify licenses and certifications that qualify individuals to perform specific duties (e.g., ICS4ICS Certifications) and ensure receiving parties recognize licensure and/or certification across geopolitical boundaries.
* **Protocols for Interoperable Communications**: Pre-arranged communication frequencies and procedures are critical for effective execution. Identify the overarching requirement for ensuring the necessary level of voice and data communications.
* **Tort Liability and Indemnification**: Specify how parties will address tort liability. For mutual aid purposes, indemnifying the person or jurisdiction or holding them harmless is a way to address liability concerns. State laws differ on tort claims, volunteer protection, Good Samaritan protection, and other incident response factors. Effective mutual aid agreements contain provisions concerning liability and indemnification to protect the parties and responders.
* **Insurance**: Address the parties’ responsibilities to provide insurance coverage.
* **Workers’ Compensation**: Address how parties will respond to workers’ compensation coverage and claims, including those from private sector, service providers, and other organization employees and volunteers.
* **Deployment Notification**: It is a best practice to include acceptable deployment notification protocols and documents in mutual aid documents to discourage unrequested resources. This section should address the documentation that will be considered official authorization to deploy, such as workorders, or travel authorizations citing a specific purpose. **W/O Clarification**
* **Reciprocity/Reimbursement**: Mutual aid agreements must specify how the receiving party will compensate the sending party.
* **Termination**: Specify how and when parties may terminate the agreement and the notification time period. Documenting this information minimizes cost and risk to all parties.
* **Dispute Resolution**: Include methods and timelines for personnel to make, process, and investigate complaints, and define the dispute resolution process. This includes how personnel make formal complaints, the adjudication method, timeframes for each step, and the implementation of resolution.
* **Modification and Amendment Management**: Identify the methods and timelines for the periodic review of the agreement by all parties, the process for parties to propose modifications or amendments to the document, and the process for approving changes.
* **Operational Plan and Procedures Requirements**: Specify requirements concerning the development of a mutual aid operational plan, including procedures, the timeline for completion, and the process for approving and implementing the plan. This may include procedures for how mutual aid resources and personnel who were mobilized to support an incident continue under the operational control of their day-to-day leaders. **W/O Clarification**
* **Supplemental Information**: Other information needed to define how the requesting party and the mutual aid provider will work together

*For more details, see Section III. Key Elements of Mutual Aid Agreement of:* [*National Incident Management System - Guideline for Mutual Aid (fema.gov)*](https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf#:~:text=The%20National%20Incident%20Management%20System%20Guideline%20for%20Mutual,entering%20into%20a%20mutual%20aid%20agreement%20or%20compact.) *from November 2017.*

## Attachment #2 - Mutual Aid Operational Plans

The subsections present key characteristics and components of effective mutual aid operational plans:

* Implementation, Schedule, Training, and Exercises: The mutual aid operational plan should include a schedule of training and exercises to validate the concepts and actions in the mutual aid operational plan prior to implementation.
* Identifying Mutual Aid Resources: Entities use various mechanisms to organize, develop, train, and exercise certain response and recovery resources prior to an emergency or disaster.
* Inventorying Resources: Include procedures to identify the immediate and future resource needs and priorities of the incident, including what and how much is needed, where and when it is needed, and who will be receiving or using it, based on incident response experience and specific damage assessments.
* Mobilizing Resources (Request, Dispatch, and Response): Describe the process for making resource requests, dispatches, and responses through mutual aid, such as formal requests from emergency operations center to emergency operations center for specific resources, or emergency-in-progress notifications by dispatchers regarding law enforcement pursuit of suspects spanning jurisdictional borders.
* Performance Criteria and Metrics: Parties establish performance criteria and metrics during the development of the mutual aid operational plan. Metrics may include size, quantity, essential elements, set of conditions or processes, personnel specifications, equipment, and team makeup. During preparation, parties document general performance criteria and metrics in mutual aid agreements and participate in developing resource typing documents.
* Management and Coordination: Provide a protocol for integrating mutual aid resources into the management and coordination structure.
* Engagement Rules: Describe the rules for how outside resources get to the scene and accomplish missions.
* Credentialing: Include details on incident personnel credentialing processes. Credentialing means providing documentation, typically badges or identification cards, which verify an individual’s identity and qualifications to fulfill an incident-related position.
* Health and Safety: The dangers and environmental hazards that responders may encounter during the incident dictate protocols for health and safety.
* Voice and Data Interoperability: Transmission of data in a common format enables sending and receiving parties to share pertinent information.
* Documentation and Reporting: Include standardized protocols for documenting and reporting procedures to help parties maintain situational awareness and give personnel access to critical information.
* Demobilizing Resources: A best practice is to include demobilization guidance in mutual aid operational plans to detail the process for demobilizing resources.