ICS4ICS
Incident Command System
for Industrial Control Systems

Delegation-of-Authority ICS4ICS Procedure Template

Instructions

The following are suggestions about how you can complete this template that is designed to establish Delegation of Authority (DOA) to empower the Incident Commander to declare an incident and have sufficient financial authority to fund incident response efforts:

- Work with C-Level executive team to grant all potential Incident Commanders with the authority to declare an incident and sufficient financial authority to fund incident response work expenditures
  - This must include the Primary, Secondary, and Tertiary Incident Commanders
  - The funding authority may be temporary DOA that gets activated once an incident is declared

Disclaimer

ISA, 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 help your company establish Delegation of Authority (DOA) to empower the Incident Commander to declare an incident and provide them sufficient financial authority to fund incident response efforts.

Situation Trigger

Before an incident occurs, the C-Level executive team must grant all potential Incident Commanders the authority to declare an incident and sufficient financial authority to fund incident response activities.

Escalation

The Security Operations Center or Computer Incident Response Team will escalate to an authorized Incident Commander who has the authority to declare an incident. After the Incident Commander declares an incident, they may need to contact the appropriate Finance person (e.g., CFO) to activate temporary DOA so they have sufficient financial authority to fund incident activities.

Notification

After the Incident Commander is notified and decides to declare an incident, they may request that the notification tool/process is used to contact the appropriate finance staff (e.g., CFO) who can update the financial systems to invoke the temporary DOA required for the Incident Commander to have sufficient financial authority to fund the incident.

Delegation of Authority (DOA)

C-Level team (who may be the Crisis Management Team) must formally perform Delegation of Authority (DOA) to empower primary, secondary, and tertiary Incident Commanders to do the following:

- Declare an Incident
    - Declaring an incident commits the company financially including cyber insurance declaration fee, declaration fee from service provider who support the company during the incident, and potentially in other parties have declaration fees.
    - Declaring an incident also starts the clock for government reporting depending on the specific reporting rules defined in laws and regulations.
- Provide sufficient financial authority to fund incident response activities
    - The Financial DOA authority should be set at a sufficient amount to ensure the Incident Commander can commit funds needed to perform incident response activities.
    - Some Incident Commanders (Primary, Secondary, Tertiary) may have sufficient financial authority. Other Incident Commanders may not have sufficient financial authority so they would need temporary Financial DOA that can be invoked after an incident is declared.
    - If the Incident Commander doesn't have sufficient financial authority, they will have to engage C-Level staff periodically to gain sufficient financial authority.

The C-Level team may want to review and approve the guidelines for declaring an incident. There is a separate procedure that defines these guidelines for declaring an incident.