ICS4ICS
Incident Command System
for Industrial Control Systems

Escalation-Notification-Declaration
ICS4ICS Procedure Template

Instructions

The following are suggestions about how you can complete this template that is designed to establish processes for escalation of cyber incidents, notification of ICS4ICS team members, and declaration of an incident:

- Develop an escalation procedure that defines when a cyber incident should be escalated from the Cyber Security (Computer Incident Response or Security Operations Center) OR OT staff to a designated Incident Commander
- Identify who and how notification processes will be executed which are designed to contact staff who need to mobilize to respond to the incident
- Document Declaration procedures the Incident Commander can used to decide to declare an incident and the subsequent steps required after notification
- Test this Escalation-Notification-Declaration Procedure and update as appropriate

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 processes for escalation of cyber incidents, notification of ICS4ICS team members, and declaration of an incident.

Situation Trigger

The Computer Incident Response Team (CIRT) will escalate cyber incidents that meet specific criteria to a designated Incident Commander who can determine if they will declare an incident. The notification process and/or tools will be used by the CIRT to notify an authorized Incident Commander and the process will be used to notify the ICS4ICS team members if the Incident Commander declares an

incident. The Incident Commander uses clearly defined criteria to determine if they will declare an incident.

Escalation

The Security Operations Center and Computer Incident Response Team must have procedures defining when and how to escalate events that may be declared as incidents by an authorized Incident Commander. This is one possible flow of how escalation may occur:

- The Security Operations Center (SOC) monitors all events. The company typically uses Security Information and Event Management (SIEM) solution to receive messages (events) from various company IT and OT systems. The SIEM helps the SOC focus on events that may be a threat to the company. The SOC will manage most of these events because they are known events that can easily be resolved. The SOC will escalate events that are new with unknown risks and/or appear to be a threat to the company.
- There may be a team that performs further analysis of the event which will become the Computer Incident Response Team (CIRT) if an incident is declared. This function may be performed by the SOC for small companies that don't have a CIRT.
- After further investigation a decision will be made to notify the appropriate manager, likely in the cybersecurity and/or OT organization manager. There may be multiple layers of more senior managers that may need to be notified before notifying an authorized Incident Commander. For example, the SOC and CIRT supervisor/manager may need to be contacted first to confirm the results and authorize notification to the next higher-level manager in the organization. The CISO, CIO, and/or another C-level people may be contacted before the Incident Commander is notified to declare an incident.
- A decision will be made to contact an Incident Commander who has the authority to declare an incident.
- The various managers and C-level staff, and the Incident Commander will be notified using the company Notification procedure.

Notification

An authorized Incident Commander will be notified and if they declare an incident staff who are needed to fill role in the ICS4ICS Team will be notified using the Notification procedure and/or tool which will include the following:

- A notification tool can be selected which will help manage the data required to perform the notification processes which are described in the subsequent bullets
    - You can search on the term “Emergency Notification System” in a web browser to find numerous commercial notification solutions
- A notification tool or manual process should include the following capabilities:
    - Data required in a notification process/tool:
        - Organization roles of people who would need to be notified
        - Primary, Secondary, and Tertiary contact information for each person who can perform each role
        - Contact information must include: name of person, their text phone number (cell), their voice phone number (home), their email address, and/or any other contact methods
        - Work Groups of roles who would be contacted as a group
            - For example, several roles would be part of the initial ICS4ICS team after an incident is declared
    - The process/tools would perform these functions:
        - Ability to trigger contact of all roles that are part of a Work Group (e.g., ICS4ICS core team members)
        - Contact the primary person from the list for a role using the various contact methods (e.g., cell phone, landline, email, etc.)
            - Typically, there would be a default time (e.g., 5 minutes) before trying the next contact method if the individual doesn’t respond
        - Contact the secondary and then tertiary person in the role using the same method, if the primary person doesn't respond after exhausting each of the contact methods
        - Create a report showing who within each role has responded to confirm they received the notification
            - Identify those roles that had no one respond so the Incident Commander can make a decision about filling these positions

Declaration

A designated Incident Commander is the only person who can declare an incident. C-Level staff (who may be the Crisis Management Team) must formally perform Delegation of Authority (DOA) to empower primary, secondary, and tertiary Incident Commanders. A designated Incident Commander will be notified after the Computer Incident Response Team (or Security Operations Center) escalates an event to them requesting them to consider declaring an incident. This is the type of criteria a company should document to help the Incident Commander to determine if declaring an incident is appropriate:

- Any event that is disrupting normal business operations
- Any event that appears to be a threat to company IT and/or OT environments
- Any event that has unknown attributes that may present a significant risk to the company or IT environment or OT systems
- An event the Incident Commander deems appropriate to declare an incident