

MINNESOTA INFORMATION SHARING AND ANALYSIS CENTER MN-ISAC

A public-private collaboration

Summary and Overview

This document outlines rules for the Minnesota Information Sharing and Analysis Center (MN-ISAC). These processes are intended to:

- Establish information sharing and analysis between businesses in Minnesota, particularly those that are a part of the critical infrastructure of the United States, or critical to the local, regional or state economy
- Support significant information sharing and coordination between officials in Federal and State & local governments.

Specifically included in this document are roles for private company representatives for these information sharing, analysis and emergency management activities:

- Roles/Administrative Rules
- Activation
- Notification
- Information Analysis
- Action Plan

Roles/Administrative Rules

Roles

The following positions are required to administer and facilitate the function of the Minnesota Information Sharing and Analysis Center (MN-ISAC):

Designated Team Lead

- Volunteer position
- Coordinates regular information-exchange meetings
- Activates and facilitates MN-ISAC analysis meetings
- Obtains volunteer commitment for other roles

Steering Committee Member

- Volunteer position
- Represents Critical Infrastructure organization within Minnesota
- Commitment to participation in planning and coordination meetings as well as contribution to planning, writing and coordination efforts
- Acts as liaison to own company and others within same sector, as possible

Public-Sector Roles

- Public Sector Participants act as liaison to their respective organizations.
- They may be tasked or constrained in this effort by those roles.

Critical Infrastructure Members

- Volunteer position
- Provides perspective of own company, and where possible, specific infrastructure sector
- Acts as liaison to local sector organizations and their critical infrastructure ISAC

Rules

1. MN- ISAC participants agree to adhere to all of these rules.
2. The participants believe that testing of communication and assessment process is key effective deployment if a crisis were to occur. Participants agree to participate in testing and scenario activities.
3. Participants will need to provide point-of-contact details for many of the processes. All participants agree to keep their contact information as current as possible.
4. Security is critical to the effective deployment of the MN- ISAC. Participants agree to secure all information relating to the MN- ISAC.
5. Federal, as well as State & local government officials should safeguard all private business information and treat such materials as business proprietary information, and mark such documents accordingly – such as with “For Official Use Only (“FOUO”). These include any record of discussions.
6. All participants agree to treat discussions associated with each of these processes as confidential.
7. Participants agree to facilitate each of the MN- ISAC to the fullest extent possible.

General Information Sharing

Protocol for sharing and analyzing information that is not immediately related to threats or incidents will be shared using the following protocol:

- Team Lead will maintain responsibility for these guidelines
- MissionMode will be the primary information sharing tool
- Participants will share information they feel is relevant to other participants or may provide public sector participants with a better ability to aggregate data relative to vulnerabilities and threats
- MissionMode alerts and the email distribution list will be used sparingly.
- "Reply-All" should be avoided unless time constrictions and severity of message indicate this is the best method to communicate

Event Activation of MN- ISAC

The Minnesota Information Sharing and Analysis Center Designated Team Lead (MN- ISAC Lead) or his/her alternate or designee has the authority to activate this plan. At a minimum, this plan will be activated in response to any incident that:

- Causes widespread damage within a small geographic area.
- Presents a significant risk of disruption of the economic infrastructure of Minnesota or the metropolitan area.

Notification Protocol

Once an incident occurs, or at the direction of the MN-ISAC Lead or participants, the following process will be implemented.

1. Using MissionMode, the Designated Team Lead will send an alert to all MN- ISAC participants.
2. The teleconference will take place 30 minutes from the completion of this notification.
3. If event has already impacted a large geographic area or is expected to gain media attention, all MN- ISAC participants are required to attend the Information Analysis meeting.
4. All MN- ISAC participants gather initial information from their respective areas of responsibility.
5. All MN- ISAC participants join Information Analysis Meeting via the Situation Room Bridgeline.

Information Analysis Meeting

MN- ISAC participants will communicate and interact via a teleconference bridge line and email/web updates.

VEOC Numbers	
Line 1 (Primary - 50 ports) Participant Code	To Be Determined
Line 2 Participant Code	To Be Determined

Objectives

The purpose of this meeting is to quickly gather:

- Known impact
- Scope of threat (How bad can it get?)
- Interaction with public emergency management, up to and including a seat at the Homeland Security and Emergency Management state emergency operations center (EOC).
- State and likelihood of escalation (Is it getting worse and how fast?)

Protocol

In order to accomplish these goals in a timely manner, the following meeting protocol will be followed:

1. Designated team lead will summarize and communicate current incident situation.
2. Each MN- ISAC participant will provide a brief report including initial assessment of the impact of the event from their area of expertise, issues for other team members, and planned course of action.
3. Incident Coordinator will open meeting for brief group discussion.
4. Incident Coordinator will summarize information gathered during call and detail Action Plan to ensure accuracy.
5. Need for next meeting and time will be set.

Action Plan

Once core team members have discussed known information, an Action Plan is determined.

Measures to be included:

- Authority confirmation
- Scope of response
- Prioritized response actions
- Coordination of Update Meeting

Update Meeting(s)

This involves a discussion of events between team members. The update is designed to quickly incorporate information about a developing incident. The information sought:

- Status update
- Necessary revision to the Action Plan
- Coordinate next update

Questions:

Chris Terzich
Incident Management
Wells Fargo & Company
612-667-7993
612-685-3688 (*NEW* cell)

Christopher.L.Terzich@Wellsfargo.com