

MINNESOTA INFORMATION SHARING AND ANALYSIS CENTER MN-ISAC



A public-private collaboration

Summary and Overview

This document provides a model for the partnership of the private critical infrastructure sectors and government entities for the purpose of protection and resilience of the regional and national economy. A company may be critical to the local or state economy without being critical to the Nation. For this group, participation will be based on criticality at any level between large urban areas and the Nation. A large employer, such as Target, may be critical to the Twin Cities, but not, as a retailer, critical to the Nation. Specifically, this document outlines rules and operational procedures 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 infrastructure¹ of the United States, or critical to the local, regional or state economy
- Create the interface and structure by which information sharing and coordination between critical infrastructure organizations and officials in Federal and State & local governments

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

- Administrative Rules
 - Roles
 - Participant rules
- Operational Rules
 - Ongoing Information Sharing (Green)
 - Active Monitoring/Partial Activation (Yellow)
 - Crisis Response (Red)

Administrative Rules

Roles

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

ISAC Chair (an alternate also appointed)

- Volunteer position selected by Governance Committee
- Coordinates and facilitates regular information-exchange meetings
- Ensures scheduling and credentialing of MN-ISAC Members within Minnesota Emergency Operations Center (EOC)
- Responsible to act as liaison to Minnesota Critical Infrastructure Working Group or other Minnesota Homeland Security functions as necessary

¹ Section 1016(e) of the USA PATRIOT Act of 2001 defines critical infrastructure sectors.

Governance Committee

- Volunteer position filled by Critical Infrastructure Member
- Commits to providing leadership and support in the operation of the Minnesota ISAC
- Represents a critical infrastructure sector
- Coordinates for other members of that sector on in all issues related to the Minnesota ISAC
- Review of additional participants

Critical Infrastructure Member

- Volunteer position
- Represents organization in all issues related to Homeland Security (e.g., physical and data security, business continuity planning, communications (PR), property management, business management).
- Represents a critical infrastructure organization
 - One of the 14 critical infrastructures of the United States
 - One of the top 25 businesses in the Minneapolis/St Paul MSA² or Minnesota
 - A large employer (5,000+) in a single metropolitan area
 - Owner or operator of a "high concentration" building of 2,000 occupants and/or 30+ stories
- Provides assessment of threat/event from perspective of his/her business
- Acts as liaison to businesses within same sector
- Participates directly in Minnesota Chapter of Infragard
- Organizational participation in sector ISAC (if applicable)
- Attendance at monthly teleconferences and quarterly in-person meetings
- Organizational participation in staffing of Minnesota EOC as necessary
- Participation in virtual MN-ISAC through subscription to MissionMode

Public-Sector Roles

- Participates directly in Minnesota Chapter of Infragard
- Organizational participation in sector ISAC (if applicable)
- Attendance at monthly teleconferences and quarterly in-person meetings
- Participation in virtual MN-ISAC through subscription to MissionMode
- Review of additional participants
- Public Sector participants will adhere to all rules and process, except where their official duties supercede participation in this group and function (i.e., National Incident Management System, Federal Response Plan, etc.).

Business Association Participants

- Volunteer position
- Participates directly in Minnesota Chapter of Infragard
- Organizational participation in sector ISAC (if applicable)
- Provide liaison to represented association and members
- Act as single point of contact for association (alternates may be established)
- Participate individually in Infragaard (if applicable)

² Metropolitan Statistical Area (<http://www.census.gov/population/estimates/metro-city/99mfips.txt>)

Participant Rules

1. MN- ISAC participants agree to adhere to all of these rules.
2. The participants believe that regular communication; along with an assessment and response process are key to effective deployments if a crisis were to occur.
3. Participants agree to participate as defined in 'Roles'.
4. 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.
5. Security is critical to the effective deployment of the MN- ISAC. Participants agree to secure all information relating to the MN- ISAC. Participants will not distribute information except within their own organizations and as defined in 'Roles'.
6. 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. Except where there is a regulatory requirement to provide information, all information within the MN- ISAC is voluntarily submitted to government participants and thus is expected to receive protection from disclosure under the provisions of the Critical Infrastructure Information Act of 2002³.
7. All participants agree to treat discussions associated with each of these processes as confidential.
8. Participants agree to facilitate each of the MN- ISAC functions to the fullest extent possible.

³ Critical Infrastructure Information Act of 2002 (CII Act)
http://www.dhs.gov/interweb/assetlibrary/CII_Act.pdf

Operational Process

The functions of the MN-ISAC can be divided into three distinct categories:

Level 1 - Ongoing Information Sharing (Green) – This describes information sharing for planning; sharing of best practices, observations and coordination information that will allow the MN-ISAC to prevent disasters and/or function better during a crisis. This operational status will coincide with Homeland Security Advisory System⁴ levels Low (Green), Guarded (Blue) and Elevated (Yellow).

Level 2 – Active Monitoring/Partial Activation (Yellow) – This describes information sharing coordination for a specific threat or event and may involve ongoing communication of participants of the Governance Committee and/or Public Sector. This operational status will coincide with Homeland Security Advisory System⁵ levels Elevated (Yellow) and High (Orange).

Level 3 – Crisis Response (Red) – This describes continuous communication of the Governance Committee, Public Sector and all participants of the MN-ISAC in response to a specific threat or event in Minnesota. This operational status will coincide with Homeland Security Advisory System⁶ levels High (Orange) and Severe (Red).

Level 1 - Ongoing Information Sharing (Green)

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

- The MN-ISAC on MissionMode will be the primary method for sharing information.
- Alerts will typically not be sent regarding information under this level.
- Regular monthly teleconferences and quarterly in-person meetings will also be used in this level.

Level 2 - Active Monitoring/Partial Activation (Yellow)

Protocol for sharing and analyzing information that is directly related to threats or incidents as determined by Governance Committee members. At a minimum, in response to any event 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.

Any governance committee member may activate this level based on need within a specific area or sector.

Communication during this level will use the following protocol:

- The MN-ISAC on MissionMode will be the primary method for sharing information

⁴ Homeland Security Advisory System - <http://www.dhs.gov/dhspublic/display?theme=29>

⁵ Homeland Security Advisory System - <http://www.dhs.gov/dhspublic/display?theme=29>

⁶ Homeland Security Advisory System - <http://www.dhs.gov/dhspublic/display?theme=29>

- An Alert will be sent to all participants using MissionMode and including information that is known by participants.
- Any Governance Committee member is authorized to initiate Alerts.
- Teleconferences may be used as well, as required or requested by Governance Committee measures
- Messages will contain the following structure:
 - Known impact
 - Scope of threat (How bad can it get?)
 - State and likelihood of escalation (Is it getting worse and how fast?)
 - Resources needed or available

Level 3 - Crisis Response (Red)

Protocol for sharing and analyzing information that is directly related to threats or incidents as determined by Governance Committee members. At a minimum, in response to any event that:

- Homeland Security Advisory System level Severe determined by the Department of Homeland Security
- Department of Homeland Security (FEMA) disaster declaration for a majority of metropolitan counties
- Other activation of the Minnesota EOC

Communication during this level will use the following protocol:

- A Governance Committee member will staff the Minnesota EOC (see Appendix 1 for Roster and Procedures)
- The MN-ISAC on MissionMode will be the primary method for sharing information
- Alert will be sent to all participants using MissionMode and including information that is known by participants.
- Governance Committee member within state EOC will be primary issuer of Alerts.
- Teleconferences may be used as well, as required or requested by Governance Committee measures
- Messages will contain the following structure:
 - Known impact
 - Scope of threat (How bad can it get?)
 - State and likelihood of escalation (Is it getting worse and how fast?)
 - Resources needed or available

Appendix 1 – Procedures for Access to Minnesota Emergency Operations Center (TBD)
Appendix 2 – Roster and calendar for MN- ISAC staffing of Minnesota Emergency Operations Center (TBD)