MS-ISAC

MULTI-STATE Information Sharing & Analysis Center™

A DIVISION OF CENTER FOR INTERNET SECURITY

MS-ISAC Membership Overview

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort based on a strong partnership with the National Cyber Security Division within the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. The MS-ISAC has built and nurtured a trusted environment of collaboration and cooperation that is improving the cyber posture of SLTT governments.

Membership in the MS-ISAC entitles you to the following services:

Member Benefits

- **Incident response resources**
  - A dedicated team is available 24/7/365 to assist Members with malware analysis, forensics, code analysis and mitigation recommendations
- **Cyber security advisories**
  - Critical, timely alerts are distributed on new and emerging threats and vulnerabilities
- **Notifications regarding potential compromised systems**
  - Through its relationships with federal partners and other intel sources, including its own intelligence, the MS-ISAC is able to correlate data and contacts Members when it becomes known their systems may have been compromised
- **Training discounts and opportunities**
  - The MS-ISAC negotiates discounts on behalf of all SLTT governments, saving as much as 85% off the commercial price, providing cost-effective access to the training that governments need most
- **Daily cyber tips feed**
  - Tips of the day highlight good cyber practices and provide guidance on how to avoid the latest threats
- **Monthly cyber security newsletters**
  - Two-page, non-technical bulletin focused on current topics and are easily brandable for you to send to your organization or constituents
- **Bi-monthly cyber security webcasts**
  - National webcasts are offered featuring experts who discuss the latest cyber issues and explain how to address them in easy to understand language
- **Monthly Member webcast meetings**
  - One-hour briefings are conducted that provide a chance to learn about the latest cyber incidents, national cyber security initiatives, special report-outs from Members, as well as the latest training and procurement opportunities

- **Emergency conference calls to brief Members on major threats or reports of cyber security incidents**
    - These conference calls bring all Members together to discuss major incidents and brief out on details
- **Access to secure portals for emails and document sharing**
    - The MS-ISAC has a compartment on the US CERT Portal that hosts a library of cyber security resource documents and enables secure email
- **Cyber security alert level status map for each state on MS-ISAC secure portal**
    - A key tool for understanding at a glance the cyber security status of the nation
- **Monthly calls for analysis regarding vendor patch releases**
    - An opportunity to participate in technical discussions regarding patches and updates
- **Participation in cyber security exercises**
    - The MS-ISAC has participated in federally sponsored cyber security exercises and acts as a voice for SLTT governments in planning meetings
- **Customized Annual Cyber Security Awareness Month material**
    - The MS-ISAC develops and distributes educational materials (print and digital) to Members for branding and distribution
- **Annual in-person Membership meeting**
    - A tremendous opportunity to meet MS-ISAC colleagues from across the country, participate in discussion groups, and learn from experts in the cyber security industry, federal agencies, Fortune 500 companies, and others
- **Fee for services**
    - The MS-ISAC can provide network monitoring, vulnerability scanning, and penetration testing as a fee for service offering

Member Responsibilities

In order to achieve a higher state of readiness and resilience to help protect our critical information, each MS-ISAC Member understands that the following principles of conduct will guide their actions and agree to the following:

- To share appropriate information between and among the Members to the greatest extent possible
- To coordinate across each of the critical sectors to reduce traditional stovepipes and other barriers in order to foster our collective mission
- To recognize the sensitivity and confidentiality of the information shared and received
- To protect all sensitive and confidential information received from other Members by taking all necessary steps at least as great as the precautions each Member takes to protect its own confidential information
- To transmit sensitive data to other Members only through the use of agreed-upon secure methods
- To take all appropriate steps to help protect our Critical Infrastructure

To take full advantage of all the MS-ISAC has to offer, Members are expected to have had their government sign a Membership Agreement. This agreement simply puts in place protocols for the sharing of information between the Member's government and the MS-ISAC (i.e. the MS-ISAC will protect any information the Member shares, and the Member will protect any information the MS-ISAC

shares). These two requirements go hand in hand, as requiring a Membership Agreement allows Members to feel more confident that when they share information, it will be shared in accordance with pre-approved protocols. Additionally, to make it easier to discover system compromises and promptly notify Members, we are requesting that all Members share their public facing IP address ranges. This can be provided on the Membership contact sheet included with this document.

Reporting an Incident and Requesting Assistance

Members can take advantage of the MS-ISAC 24/7/365 Security Operations Center (SOC) and Computer Emergency Response Team (CERT). Examples of events to report to the MS-ISAC include the following:

- Unauthorized access to information
- Defacement of a government web page
- Unauthorized use of system privileges
    - Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Compromised password(s)
- Disruption or attempted denial of service (DoS)
- Unauthorized use of a system for the transmission, processing or storage of data.
- Execution of malicious code, often expressed as malware
    - Viruses, Trojans, worms, botnets
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

MS-ISAC Workgroups

All Members are encouraged to join a workgroup. The workgroups share ideas, generate recommendations and produce deliverables to support the MS-ISAC and Member-related programs. Participating in a workgroup offers a great opportunity to lend your voice to a national organization, learn about other government's initiatives, and network with your peers. Workgroups meet monthly or bi-monthly via conference call and in person once a year.

Below is a list of MS-ISAC workgroups:

Cyber Security Metrics and Compliance: Focused on recommending and implementing methodologies to help states with cyber security metrics and compliance inventory, assessment and audit of their cyber security assets.

Cyber Exercise: Focused on facilitating cyber exercise programs for MS-ISAC and states' participation.

Education and Awareness: Focused on development of new--or identification of existing--cyber security education, awareness and training content for states and localities. This includes participation in National Cyber Security Awareness Month.

Legislative Awareness: Focused on tracking all major legislation, rules and regulations across the country relating to cyber security issues, and relevant cyber security.

New Member: Focused on serving as a key resource for the MS-ISAC in developing best practices for identifying new Members across the SLTT governments domain, developing and distributing new methods for enhanced Member engagement, as well as serving as a forum for new ideas on disseminating MS-ISAC information.

Services: Focused on strategies for operational cyber security initiatives, both within the MS-ISAC, as well as for SLTT governments. This includes recommendations of standards and procedures for incident reporting and response.

Procurement: Focused on assisting SLTT governments in identifying strategies for procurement of goods and services related to cyber security initiatives; facilitating opportunities for state and local joint procurement as well as identifying and recommending available grant opportunities.

Contact Information

MS-ISAC 24/7/365
Security Operations Center:
1-866-787-4722
soc@msisac.org

MS-ISAC Headquarters:
1-518-266-3460
info@msisac.org

Office hours are 8:30am – 5:30pm Eastern
31 Tech Valley Drive
East Greenbush, NY 12061