



## Center for Internet Security Multi-State Information Sharing and Analysis Center (MS-ISAC)

### Charter

---

#### **Overview and Mission**

The Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the Center for Internet Security, is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments

The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, territorial and tribal governments. Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security (DHS) are the keys to success.

The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from its members and a two-way sharing of information between and among its members in order to protect, defend, detect, respond and recover from attacks on public and private critical infrastructure (CI). The MS-ISAC's 24-hour watch and warning center provides real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the nation's SLTT government cyber domain.

The MS-ISAC comprises representatives from all 50 states, the District of Columbia, as well as U.S. territories and local governments. The MS-ISAC has built and nurtured a trusted environment between and among our nation's state, territory and local governments by providing valuable information and lessons learned on cyber threats/exploits, vulnerabilities, consequences, and incidents, and direct assistance with responding to and recovering from cyber attacks and compromises.

**"This [cyber] threat is one of the most serious economic and national security challenges we face as a nation.**

**"We will work with key players – including state and local governments and the private sector– to ensure an organized and unified response..."**

President Obama, May 29, 2009

**"To help build situational awareness related to the information and communications infrastructure, the Federal government should leverage existing resources such as the Multi-State Information Sharing and Analysis Center ..."**

60-Day Cyberspace Policy Review  
May 2009

The MS-ISAC works closely with the DHS and is recognized as the national ISAC for the states and local governments to coordinate cyber readiness and response.

The MS-ISAC also works closely with other organizations, such as the National Council of ISACs, the National Governors' Association, and the National Association of State Chief Information Officers, as well as other public and private sector entities to build trusted relationships to further enhance our collective cyber security posture.

### ***Principles of Conduct***

The MS-ISAC is operationally focused and actions will be achieved through:

1. Coordination
2. Collaboration
3. Communication
4. Cooperation

As part of the membership in the MS-ISAC, in order to achieve a higher state of readiness and resilience to help protect our CI, each MS-ISAC Member understands that the following principles of conduct will guide their actions:

- (a) Agree to the above-stated common Mission;
- (b) Agree to the MS-ISAC's philosophy of collaboration and cooperation and will work collaboratively with all entities within their organization to further promote the collective mission of the MS-ISAC;
- (c) Agree to share appropriate information between and among the Members to the greatest extent possible;
- (d) Agree to coordinate across each of the critical sectors to reduce traditional stovepipes and other barriers in order to foster our collective mission;
- (e) Agree to recognize the sensitivity and confidentiality of the information shared and received;
- (f) Agree 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;
- (g) Agree to transmit sensitive data to other Members only through the use of agreed-upon secure methods.
- (h) Agree to take all appropriate steps to help protect our CI.

### ***Membership***

There shall be one category of MS-ISAC membership.

An organization shall be eligible for MS-ISAC membership provided the organization meets the following requirements:

1. It is one of the 50 States, the District of Columbia (D.C.), a U.S. Territory, or a U.S. local government entity.

- a. Membership can include individuals from both the cyber and physical security departments.
2. Executes the MS-ISAC non-disclosure agreement.

### **Definitions**

1. Member: refers to any individual from one of the 50 States, the District of Columbia, a U.S. Territory, or a U.S. local government entity who belongs to the MS-ISAC.
  - a. Principal Member: the designated individual point of contact (POC) from a state, territory or District of Columbia and the voting representatives for their state, territory or District of Columbia
  - b. Primary Local Government Member: an individual from a U.S. local government entity who serves as a full voting participant in the MS-ISAC.
2. Chair: directs the day-to-day functions of the MS-ISAC and coordinates activities and funding with the Federal Government.
3. MS-ISAC Executive Committee Member: refers to a Member who is elected by the membership to assist in governance for the MS-ISAC.
4. Formal vote: refers to an official vote for which it is announced in advance that votes will be counted. This may occur during the course of a meeting or via email balloting.

### **Representation**

1. Each state, territory and District of Columbia may appoint (2) two Principal Members (one cyber; one physical) to officially represent them on the MS-ISAC.
2. Additionally, each state/territory may identify (1) one individual from a U.S. local government entity to serve as the Primary Local Government Member.
3. A state, territory, District of Columbia or U.S. local government entity may designate as many individuals as it would like to participate as Members in the MS-ISAC, and attend meetings and functions as appropriate.
4. A roster of Members will be maintained by the Chair and each Principal Member and Primary Local Government Member will keep the information pertaining to their state/territory/District of Columbia/U.S. Local Governments' Member's updated in a secure manner on the MS-ISAC portal.
5. Meetings, except for the Annual Meeting, will be held on the last Tuesday of each month at 3:00pm Eastern, via teleconference and webcast.
6. MS-ISAC meetings are open to all levels of Members.
7. MS-ISAC Members may recommend to the Chair other invited guests to attend MS-ISAC meetings.
8. Meetings may provide opportunities for Members to make recommendations. Voting on such recommendations will be by a simple majority of the individuals participating in the vote.
9. Archives of the monthly meetings will be made available via the MS-ISAC portal.
10. The MS-ISAC Chair or designee will determine when meeting minutes and other MS-ISAC-developed documents may be released beyond the MS-ISAC membership.

### **MS-ISAC Executive Committee**

There shall be an eleven (11) member Executive Committee for the MS-ISAC. One of the Committee members is the Chair of the MS-ISAC and the remaining Committee members will be from different states/territories/District of Columbia/U.S. Local Government entities.

1. The term of Executive Committee members is three (3) years, except for the Chair.
2. Executive Committee members will be voted upon by the full MS-ISAC. Those members with the most votes will be selected for the Executive Committee. In the case of a tie, the Chair will make the selection. If a committee member leaves before the end of a term, they will be replaced with a vote during the next committee member voting process.
3. The Executive Committee will vote on matters brought to its attention coming from work groups or the members at large. Each Committee member will have one vote on matters presented by the Chair for vote by the Executive Committee, with a tie vote being broken by the Chair. A simple majority will be sufficient to carry the vote.
4. The Executive Committee will meet quarterly by phone/webcast or in person.
5. Executive Committee members are expected to be ambassadors for the MS-ISAC by promoting and supporting its mission, by participating in reporting and other activities of the MS-ISAC, and by encouraging other Members to participate in the activities of the organization.

### ***MS-ISAC Deliverables***

(This is a dynamic list to be reviewed periodically by the MS-ISAC.)

- operate a 24x7 cyber security center
- provide two-way sharing of information and early warnings on cyber security threats
- provide trending and other analysis for security planning
- distribute cyber security advisories and bulletins
- provide cyber incident response to MS-ISAC Members
- implementation of cyber incident reporting protocols
- establishment of common cyber alert level map and protocols
- facilitation of multi-state procurement efforts
- participation in cyber exercises, including the national Live Wire and Cyber Storm exercises
- coordination of bi-monthly national cyber security webcasts
- co-chair of National Cyber Security Awareness Month
- issuance of white papers, monthly email newsletters, cyber security guides, training videos and other educational material
- conduct monthly Member webcast meetings and annual meetings
- maintenance of secure and public websites
- promote awareness of the interdependencies between cyber and physical critical infrastructure as well as between and among the different sectors
- work collaboratively with the public and private sectors to foster communication and coordination
- ensure that all necessary parties are vested partners in this effort

### ***Workgroups***

The MS-ISAC may appoint workgroups or subcommittees to deal with specific matters. Workgroups will be co-chaired by MS-ISAC Members and may include subject matter experts from entities that are not Members of the MS-ISAC.

### ***Document Management***

Any changes made to this charter will be done by a majority vote of the membership.

- *Original Charter Adopted October 2004*
- *Current updated version adopted September 2009*
- *Updated March 2011*