MS-ISAC Overview

(Multi State – Information Sharing & Analysis Center)

Quick Brief:

- What is an ISAC?
- Who is MS-ISAC?
- What services are available?
- Who can be a member?
- What is the cost?
- How do you join?

What is an ISAC?
(Information Sharing & Analysis Center)

- Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.
- ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

What is an ISAC?
(Information Sharing & Analysis Center)

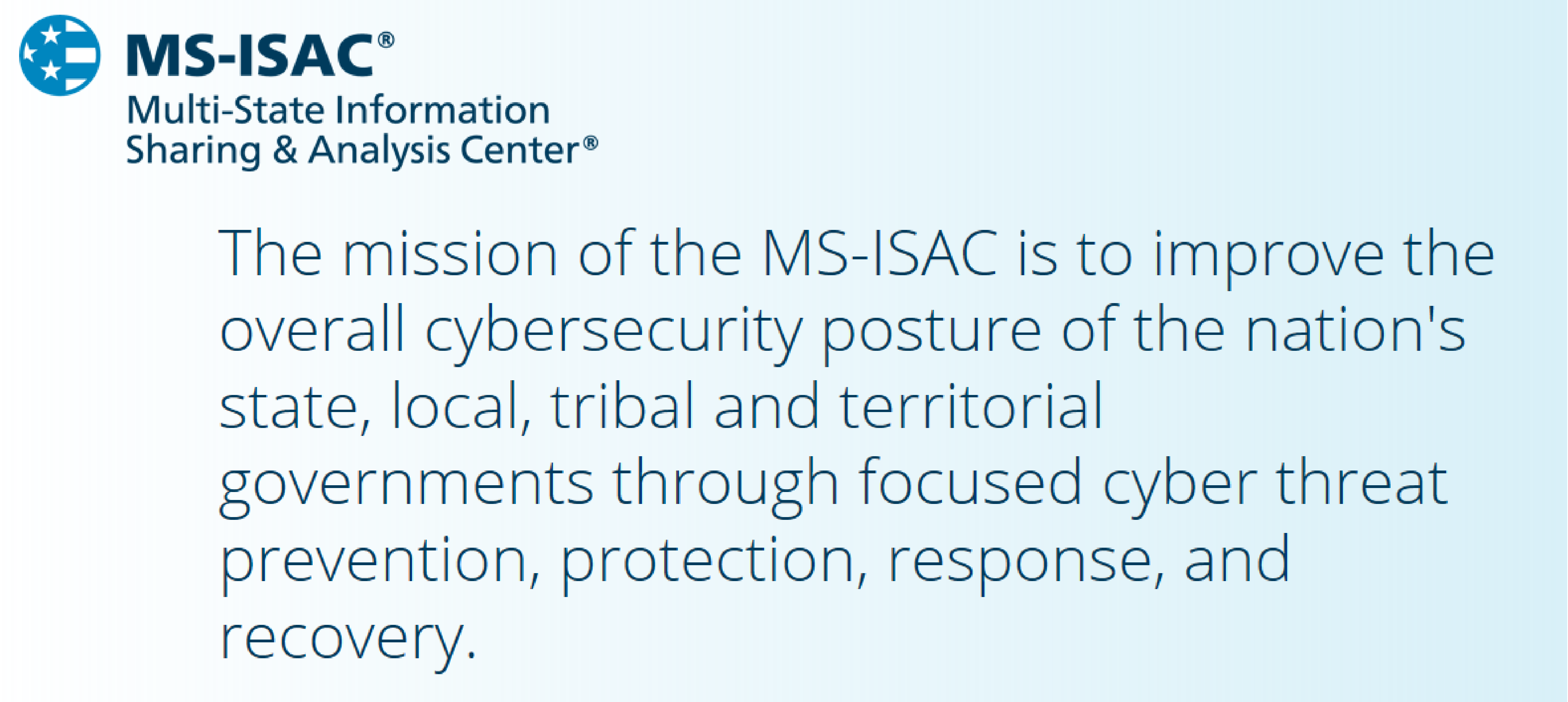
- The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities.
- Some ISACs formed as early as 1999, and most have been in existence for at least ten years

There are currently 21 ISACs

AUTO-ISAC
Automotive Information Sharing and Analysis Center
MS-ISAC
FINANCIAL SERVICES ISAC
REN-ISAC
MARITIME SECURITY COUNCIL
MARITIME ISAC
MARITIME INFORMATION SHARING & ANALYSIS CENTER
DNG-ISAC
H-ISAC
HEALTH - ISAC
National Defense ISAC
AVIATION ISAC
WaterISAC
A DIVISION OF NERC
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
HEALTHCARE READY
STRENGTHEN. SAFEGUARD. RESPOND.
NCC
Real Estate ISAC
Information Sharing and Analysis Center
Serving the Commercial Facilities Sector
IT ISAC
DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER
Surface Transportation Public Transportation Over the Road Bus
Information Sharing and Analysis Centers
24/7 Threat Warning & Incident Reporting
ONG-ISAC
RETAIL & HOSPITALITY ISAC
Elections Infrastructure ISAC™

Source: https://www.nationalisacs.org/member-isacs

Who is MS-ISAC?



MS-ISAC®

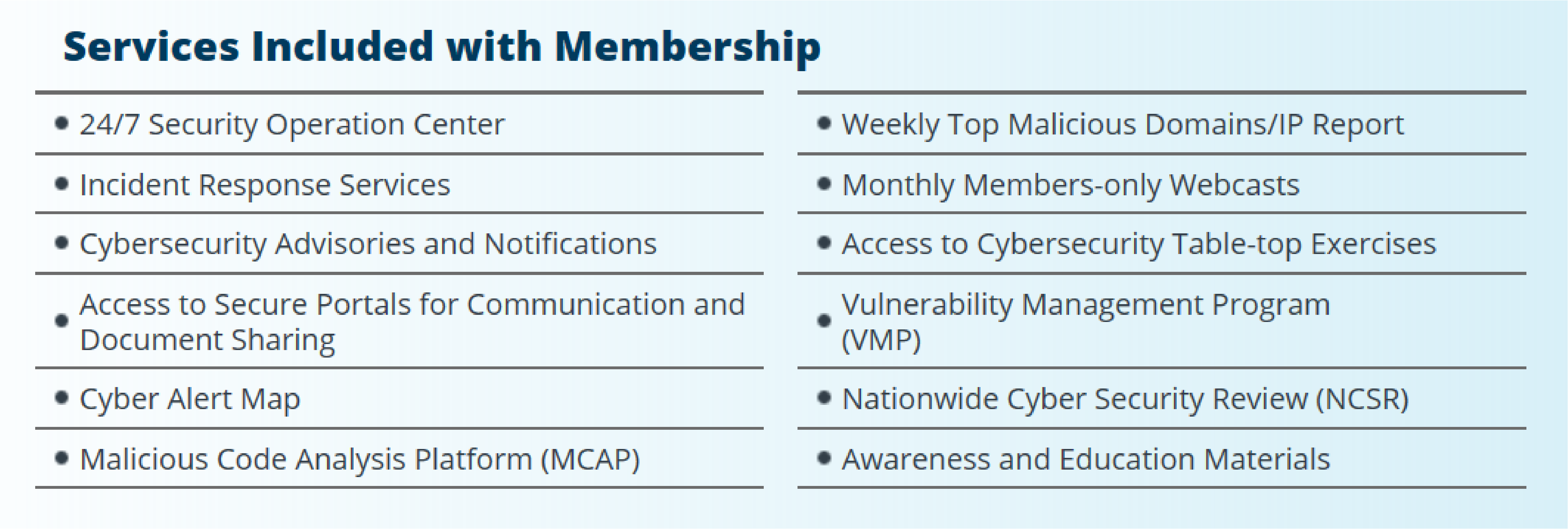
Multi-State Information Sharing & Analysis Center®

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

www.cisecurity.org/ms-isac

- The MS-ISAC’s 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response services.
- The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for SLTTs, including Chief Information Security Officers, Homeland Security Advisors and Fusion Center Directors.

MS-ISAC Services



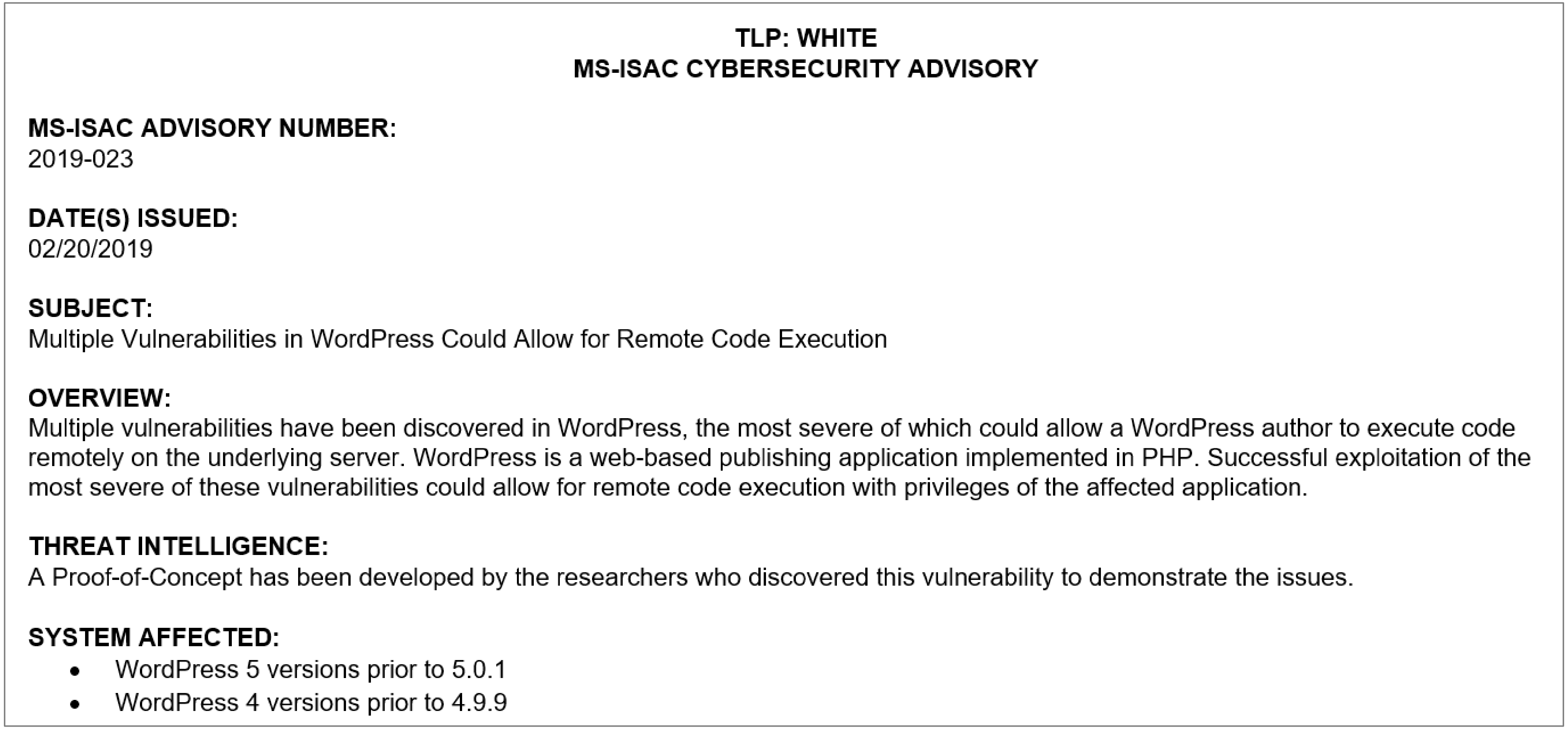
Services Included with Membership

- 24/7 Security Operation Center
- Incident Response Services
- Cybersecurity Advisories and Notifications
- Access to Secure Portals for Communication and Document Sharing
- Cyber Alert Map
- Malicious Code Analysis Platform (MCAP)
- Weekly Top Malicious Domains/IP Report
- Monthly Members-only Webcasts
- Access to Cybersecurity Table-top Exercises
- Vulnerability Management Program (VMP)
- Nationwide Cyber Security Review (NCSR)
- Awareness and Education Materials

MS-ISAC - **Advisories**

- MS-ISAC Security Operations Center (SOC) analyzes cyber threat information from a variety of sources and shares this information with MS-ISAC members when necessary.
- Information can include threats, vulnerabilities, exploits, attacks and compromises
- In addition to these advisories, MS-ISAC provides its members
  - weekly threat reports
  - monthly situational awareness reports
  - monthly webcasts

MS-ISAC - **Advisories**



TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2019-023

DATE(S) ISSUED:
02/20/2019

SUBJECT:
Multiple Vulnerabilities in WordPress Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in WordPress, the most severe of which could allow a WordPress author to execute code remotely on the underlying server. WordPress is a web-based publishing application implemented in PHP. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution with privileges of the affected application.

THREAT INTELLIGENCE:
A Proof-of-Concept has been developed by the researchers who discovered this vulnerability to demonstrate the issues.

SYSTEM AFFECTED:

- WordPress 5 versions prior to 5.0.1
- WordPress 4 versions prior to 4.9.9

MS-ISAC - **Threat Notifications**

- MS-ISAC analysts work with trusted affiliates to conduct research and gather intelligence about cyber threats (such as website defacement) targeting government or government-affiliated systems.
- Notices are sent to impacted MS-ISAC members based on predetermined escalation procedures.
- The MS-ISAC also provides recommended remediation steps and technical assistance.

MS-ISAC - Vulnerability Assessment

- For state, local, tribal, and territorial (SLTT) entities experiencing a targeted cyber threat, the MS-ISAC provides a free network and web application vulnerability assessment.
- These assessments include a manual analysis and verification of vulnerabilities discovered, prioritized remediation steps, customized reporting, and remediation support.

MS-ISAC - Malicious Code Analysis Platform (MCAP)

- MCAP is a web-based service which allows members to submit suspicious files, including executables, dlls, documents, quarantine files and archives for analysis in a controlled and non-public fashion. MCAP also enables users to perform threat analysis based on domain, IP address, URL, HASH, and various IOCs.
- MCAP users are able to obtain the results from analysis, behavioral characteristics and additional detailed information which allows users to remediate the incident in a timely manner. This communication with our members provides the MS-ISAC with the situational awareness needed to assess the malware threat characteristics facing our SLTT government entities on a national level.

MS-ISAC - **Vulnerability Management Program (VMP)**

- VMP notifies members on a monthly basis about any outdated software that could pose a threat to assets. A scripted GET request is sent to over 30,000 SLTT domains that the MS-ISAC maintains, to pull data on versioning information related to each domain.
- In order to alert members of outdated software, the MS-ISAC collects server type and version (IIS, Apache, Nginx, etc.), web programming language and version (PHP, ASP, etc.), and content management system and version (WordPress, Joomla, Drupal, etc.)
- Following the analysis and review of the information returned, data will be broken out into two categories: vulnerable and not vulnerable systems. If the system is located in the 'vulnerable' file, an associated portion of that system is not up to date. Conversely, if the system is located in the 'not vulnerable' file, the system's patch level is up to date. Systems identified as vulnerable include the CVE score and a link to the CVE.
- Members should use this monthly notification to conduct further internal analysis to ensure that Internet facing systems are patched and running the most up to date software.

MS-ISAC –
Information Sharing, Cybersecurity Awareness, and Education

- Through the Homeland Security Information Network (HSIN), MS-ISAC members can access a library of cybersecurity resources. This portal also provides contact information and allows for secure email and document sharing.

MS-ISAC –
Information Sharing, Cybersecurity Awareness, and Education

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT
U.S. DEPARTMENT OF HOMELAND SECURITY
CYBER SECURITY

- FEDVTE (https://fedvte.usalearning.gov/portal.php)

CIS® Center for Internet Security®

Secure Your Organization

CIS Controls

IT security leaders use CIS Controls to quickly establish the protections providing the highest payoff in their organizations. They guide you through a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

Secure Your Systems & Platforms

CIS Benchmarks™

Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks. They are continuously verified by a volunteer IT community to combat evolving cybersecurity challenges.

Members of MS-ISAC are eligible for a free CIS SecureSuite membership.

Who can be a member of MS-ISAC?

Membership in the Multi-State ISAC is open to employees or representatives from:

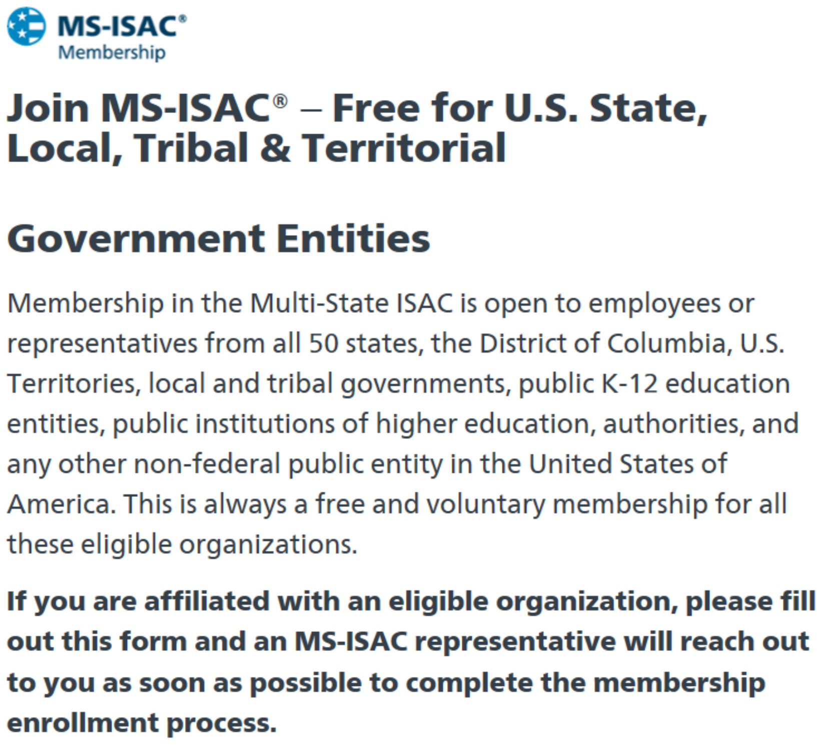
- All 50 states, the District of Columbia, U.S. Territories, local and tribal governments, **public K-12 education entities**, public institutions of higher education, authorities, and any other non-federal public entity in the United States of America.

What is the cost of MS-ISAC membership?

- This is always a **free and voluntary membership** for all these eligible organizations.

How do you join MS-ISAC?

- Visit: https://learn.cisecurity.org/ms-isac-registration



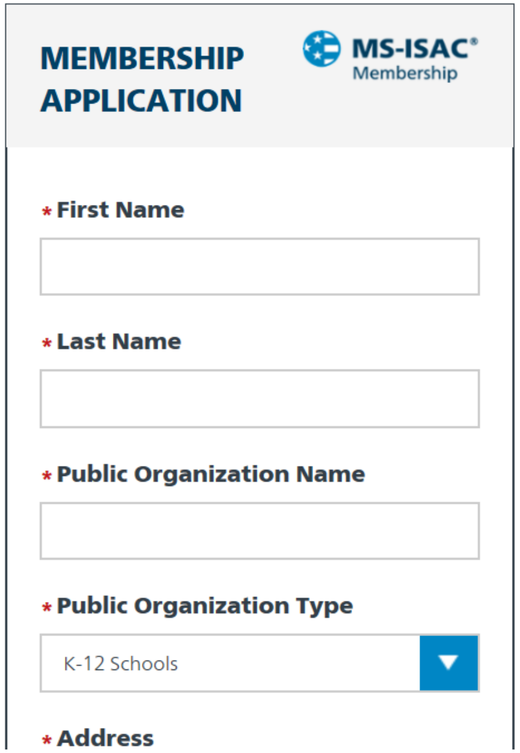
MS-ISAC® Membership

Join MS-ISAC® – Free for U.S. State, Local, Tribal & Territorial

Government Entities

Membership in the Multi-State ISAC is open to employees or representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the United States of America. This is always a free and voluntary membership for all these eligible organizations.

If you are affiliated with an eligible organization, please fill out this form and an MS-ISAC representative will reach out to you as soon as possible to complete the membership enrollment process.



MEMBERSHIP APPLICATION

MS-ISAC® Membership

* First Name

* Last Name

* Public Organization Name

* Public Organization Type

K-12 Schools ▼

* Address

Questions?

Daniel Ramirez
danramirez@esc1.net