

0194-112025

**RESOLUTION Support Wisconsin establishing a Membership with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to Cover the Cost of Membership for all State, Local, Tribal and Territorial (SLTT) Organizations.**

**TO THE WINNEBAGO COUNTY BOARD OF SUPERVISORS:**

**WHEREAS**, the Multi-State Information Sharing and Analysis Center (MS-ISAC) provides vital cybersecurity services, including 24/7 threat monitoring and incident response, to more than 18,000 state, local, tribal, and territorial (SLTT) government organizations supporting our nation's critical infrastructure including public hospitals, public utilities, K-12 school, and law enforcement; and

**WHEREAS**, local governments, especially in rural and under-resourced areas, have relied heavily on MS-ISAC's services; and

**WHEREAS**, without MS-ISAC services, government organizations are increasingly vulnerable to cyber attacks by foreign adversaries; and

**WHEREAS**, recent federal funding cuts to MS-ISAC, have significantly weakened the nation's defense against cyber threats; and

**WHEREAS**, Winnebago County joined MS-ISAC under the Single Organization Membership option on September 1, 2025, when funding ended, to continue the services Winnebago County needed to protect its infrastructure and data; and

**WHEREAS**, MS-ISAC has said the fees paid by Winnebago County will be refunded or applied to other add-on services should Wisconsin obtain membership with MS-ISAC in the future.

**NOW, THEREFORE, BE IT RESOLVED** by the Winnebago County Board of Supervisors that it supports Wisconsin establishing a Membership with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to Cover the Cost of Membership for all State, Local, Tribal and Territorial (SLTT) Organizations.

**BE IT FURTHER RESOLVED** that the Winnebago County Clerk is hereby authorized to send a copy of this Resolution to the Governor of the State of Wisconsin, all Wisconsin counties, and the Wisconsin Counties Association for consideration.

Respectfully submitted by:  
LEGISLATIVE COMMITTEE  
Committee Vote: 12-0

Fiscal Note:

Vote Required for Passage: **THREE-FOURTHS OF MEMBERS PRESENT**

Approved by the Winnebago County Executive on

November 21, 2025

A handwritten signature in black ink, appearing to read "Gordon Hintz", is written over a horizontal line. The signature is stylized with large, flowing letters.

45  
46 Gordon Hintz  
47 Winnebago County Executive  
48

# Agenda Item Report



DATE: November 18, 2025  
FROM: Jennifer Ruetten, Director of Information Technology  
AGENDA ITEM: Support Wisconsin establishing a Membership with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to Cover the Cost of Membership for all State, Local, Tribal and Territorial (SLTT) Organizations.

## **General Description:**

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides vital cybersecurity services to more than 18,000 state, local, tribal, and territorial (SLTT) government organizations supporting our nation's critical infrastructure including public hospitals, public utilities, K-12 schools, and law enforcement. Without these services, they will be increasingly vulnerable to cyber attacks by foreign adversaries.

## **Action Requested:**

Motion to recommend passage of the resolution.

## **Procedural Steps:**

County Board rule requires the Legislative Committee to recommend this resolution to the County Board, where it will require a 3/4 vote.

## **Background:**

The recent federal funding cuts to the Multi-State Information Sharing and Analysis Center (MS-ISAC), a key cybersecurity resource for state and local governments, have significantly weakened the nation's defense against cyber threats. Established in 2003 under the Center for Internet Security (CIS), MS-ISAC has been instrumental in providing 24/7 threat monitoring, incident response, and cybersecurity resources to over 18,000 state, local, tribal, and territorial (SLTT) entities. The recent \$10 million funding cut by the Cybersecurity and Infrastructure Security Agency (CISA) has led to the cessation of critical services, leaving many jurisdictions vulnerable to cyberattacks.

## **Impact on Local Governments:**

1. Increased Vulnerability to Cyber Threats - Local governments, especially in rural and under-resourced areas, have relied heavily on MS-ISAC's services, including threat intelligence sharing, incident response support, and cybersecurity tools. The loss of these services has left many jurisdictions without the necessary resources to defend against cyber threats, increasing their vulnerability to attacks.
2. Financial Strain and Resource Gaps - The absence of MS-ISAC's support has led to financial strain on local governments, as they now face the challenge of securing alternative cybersecurity resources, often at higher costs. This financial burden is

particularly challenging for smaller jurisdictions with limited budgets.

3. Disruption of Information Sharing Networks - MS-ISAC served as a central hub for information sharing among SLTT entities, fostering collaboration and coordinated responses to cyber threats. The dissolution of this network has disrupted communication channels, hindering the ability of local governments to respond effectively to cyber incidents.

Options for MS-ISAC Service Continuance:

1. The state of Wisconsin can establish a membership with MS-ISAC under the State/Territory-Wide Membership option to cover the cost for all SLTT entities in the state.
2. Winnebago County can join MS-ISAC under the Single Organization Membership option.
3. Winnebago County can separately contract with third-party vendors for all of the services that we previously had for free.

This is not just about Winnebago County. MS-ISAC is a resource that was available to any SLTT and because of this, the funding cut affects everyone. While the bottom line isn't that great for just Winnebago County, we are impacted if fewer entities choose the paid membership options. Information sharing is critical to cybersecurity defenses and fewer participants equals less information. We are only as strong as our weakest link when it comes to cybersecurity and MS-ISAC was a way for small entities to prioritize cybersecurity. For member entities, this was a crucial component to their cybersecurity posture. Lower participation in membership might also result in higher membership fees during future service renewals.

These federal funding cuts also affected the Election Infrastructure Information Sharing Analysis Center (EL-ISAC) which supported clerks through information and resources and worked to protect the election process from cyberattack.

Funding ended September 1, 2025 and Winnebago County had to choose Option 2 to continue the services that we need to protect our infrastructure and data. Should the state of Wisconsin obtain membership at a later time, MS-ISAC has stated that the fees we have paid will be refunded or applied to other add-on services.

October 1, 2025 Update:

The Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) has chosen not to renew federal funding that has supported the MS-ISAC for the past 20 years. For this reason, MS-ISAC has fully transitioned to the fee-based membership model. As a result of the loss of federal funding, member tier pricing will be adjusted to reflect the "No Federal Funding" structure.

Because Winnebago County established our paid membership prior to September 1, we did pay the lower cost as depicted in the Cost Comparison attachment and our membership is effective for 18 months before we need to renew.

**Policy Discussion:**

To have the greatest cybersecurity impact across the nation, restoration of federal funding is ideal. At a minimum, we request that the state of Wisconsin enter into the State/Territory-Wide Membership option with MS-ISAC to provide these valuable services to all SLTT entities in the state.

**Attachments:**

None



## Options for MS-ISAC Service Continuance

Service Type	Option 1 - WC costs prior to the 2025 cut in federal funding and if WI enters into a statewide agreement*	Option 2 - New pricing structure as of Sept 2025 as a single membership	Option 3 - Cost to obtain these services separately from 3rd parties
MS-ISAC Membership/Participation	\$0.00	\$4,995.00	N/A
Malicious Domain Blocking & Reporting (MDBR)	\$0.00	\$0.00	\$5,000.00
Malicious Code Analysis Platform (MCAP)	\$0.00	***Add-On	\$3,000.00
Nationwide Cyber Security Review (NSCR)	\$0.00	\$0.00	\$0.00
Cyber Threat Intelligence Reports	\$0.00	\$0.00	\$2,000.00
CrowdStrike**	\$3,300.00	\$3,300.00	\$18,000.00
<b>TOTAL</b>	<b>\$3,300.00</b>	<b>\$8,295.00</b>	<b>\$28,000.00</b>

\*Although the Statewide Membership Option information is sparse, we've heard through sources that our new cost would be similar to our prior costs if the State of Wisconsin had an agreement in place.

\*\*WC purchased this subscription through MS-ISAC under a purchase discount program.

Unclear if CrowdStrike discount will remain or change after Sept 2025.

\*\*\*Add-On price not published at this time. The total for Option 2 would be higher.







HOME / NEWS

## Multi-State Information Sharing and Analysis Center (MS-ISAC) loses federal funding

MAR 25, 2025

5 min read

### AUTHOR



**Seamus Dowdall**

Legislative Director, Telecommunications & Technology



**Paige Mellerio**

Legislative Director, Finance, Pensions & Intergovernmental Affairs | Local Government Legal Center



**Rita Reynolds**

Chief Information Officer & Managing Director, County Tech Xchange



**Emma Conover**

Legislative Assistant

### UPCOMING EVENTS

### RELATED NEWS





## Key Takeaways

The Cybersecurity Infrastructure and Security Agency has announced in recent weeks that it would withdraw federal funding for the MS-ISAC and EI-ISAC

MS and EI- ISAC offer free and low cost cyber and election security tools and technical assistance, providing crucial resources to counties with limited capacity

On March 11, the Cybersecurity and Infrastructure Security Agency (CISA) announced a \$10 million cut in funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides critical local assistance for cybersecurity threat detection and analysis resources and support. The announcement was the latest development in a series of funding cancellations from CISA that have affected multiple cybersecurity sharing regimes that support county cybersecurity readiness initiatives. In February, CISA made a similar announcement to withdraw federal support for the EI- ISAC, which provides critical cybersecurity tools and technical assistance to election offices across the country.

## What is the MS-ISAC?

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides no-cost and low cost cyber threat prevention, protection, response, and recovery for state and local governments. CISA has provided funds to support the MS-ISAC under a cooperative agreement with the Center for Internet Security for nearly 20 years. Under this contract, the MS-ISAC provides more than 17,000 state, local, tribal and territorial entities with the following no and low-cost services:

- vulnerability management programs (low-cost),
- End point protection (no-cost and low-cost),
- IP and domain monitoring,
- notifications of possible compromises,
- incident response resources,
- tools for simplifying security updates,
- secure portals for communication and document sharing,
- cyber intel advisories & alerts,
- malicious code analysis platform and
- self-assessments for cybersecurity management.

The \$10 million allocated by CISA accounted for just under half of the MS-ISAC's funding. The Center for Internet Security is reportedly reviewing which operations they will continue and which they will discontinue under a scenario of no federal support for the MS-ISAC.

## What is the EI-ISAC?

The Election Infrastructure Information Sharing Analysis Center (EI-ISAC) supports local government threat prevention for election offices. EI-ISAC members have free access to technical support, threat monitoring, election security operations centers, and trainings to bolster election security. According to the EI-ISAC website, the \$10 million cut in funding has effectively halted all operations for the program.

The EI-ISAC served as an important information sharing center, allowing election officials to share cybersecurity threat and response tactics. As elections have rapidly become more automated, county election officials have had to become cybersecurity experts in addition to election administrators. The EI-ISAC plays a unique role in cyber support and information sharing, and the loss of access to critical support staff at the EI-ISAC will have an impact on counties who do not have in-house staffing capacity and rely on EI-ISAC for up-to-date information and resources.

### How does this affect counties?

Rural and under-resourced counties have relied on free tools and technical assistance through both the MS-ISAC and EI-ISAC to bolster cyber-readiness and improve security practices at the local government level. Counties also utilize available resources from the MS-ISAC and EI-ISAC to coordinate with other localities, including cities and municipalities, on cybersecurity readiness and information-sharing. Counties support funding assistance for critical cybersecurity tools and resources required to adequately protect county security at all levels, including the cybersecurity of election infrastructures and election workers.

NACo is urging Congress to re-instate federal funding for both initiatives to preserve an information-sharing ecosystem that can support county cybersecurity readiness across critical infrastructure areas and core functions, such as in the administration of the nation's elections.

---

TAGGED IN:

TELECOMMUNICATIONS & TECHNOLOGY, ELECTIONS

---

#### COUNTY NEWS

---

## MS-ISAC: Phight the phish by learning to identify malicious emails

OCTOBER 11, 2021

[Read More](#)

### Related News



660 North Capitol Street, NW Suite 400  
Washington, DC 20001

(202) 393-6226

[Contact Us](#)

© 2025 National Association of Counties



# Multi-State Information Sharing and Analysis Center Loses Federal Funding

By National Association of Counties Staff

**Editor's note:** The Trump administration has been proposing and advancing widespread reductions to federal government spending. This article focuses on one aspect of cybersecurity funding. Visit [NACo.org](http://NACo.org) for more information about these and other cuts to federal programs and staffing.

**O**n March 11, the Cybersecurity and Infrastructure Security Agency (CISA) announced a \$10 million cut in funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides critical local assistance for cybersecurity threat detection and analysis resources and support. The announcement was the latest development in a series of funding cancellations from CISA that have affected multiple cybersecurity sharing regimes that support county cybersecurity readiness initiatives. In February, CISA made a similar announcement to withdraw federal support for the Election Infrastructure Information Sharing Analysis Center (EI-ISAC), which provides critical cybersecurity tools and technical assistance to election offices across the country and rural and under-resourced counties at no cost or low cost.

## ► What is the MS-ISAC?

The MS-ISAC provides no-cost and low-cost cyber threat prevention, protection, response, and recovery for state and local governments. CISA has provided funds to support the MS-ISAC under a cooperative agreement with the Center for Internet Security for nearly 20 years. Under this contract, the MS-ISAC provides more than 17,000 state, local, tribal and territorial entities with the following no- and low-cost services:

- Vulnerability management programs (low-cost)
- End-point protection (no-cost and low-cost)
- IP and domain monitoring
- Notifications of possible compromises

- Incident response resources
- Tools for simplifying security updates
- Secure portals for communication and document sharing
- Cyber intel advisories and alerts
- Malicious code analysis platform
- Self-assessments for cybersecurity management

The \$10 million allocated by CISA accounted for just under half of the MS-ISAC's funding. The Center for Internet Security is reportedly reviewing which operations they will continue and which they will discontinue under a scenario of no federal support for the MS-ISAC.

## ► What is the EI-ISAC?

The EI-ISAC supports local government threat prevention for election offices. EI-ISAC members have free access to technical support, threat monitoring, election security operations centers, and trainings to bolster election security. According to the EI-ISAC website, the \$10 million cut in funding has effectively halted all operations for the program.

The EI-ISAC serves as an important information-sharing center, allowing election officials to share cybersecurity threat and response tactics. As elections have rapidly become more automated, county election officials have had to become cybersecurity experts in addition to election administrators. The EI-ISAC plays a unique role in cyber support and information sharing, and the loss of access to critical support staff at the EI-ISAC will have an impact on counties that do not have in-house staffing capacity and rely on the EI-ISAC for up-to-date information and resources.



## The Impact on Wisconsin Counties

By Trina Zanow, Chief Information Officer, Department of Administration's Division of Enterprise Technology

The state of Wisconsin, along with nearly 600 local and tribal government entities in Wisconsin, including 62 county governments, are members of MS-ISAC and will be impacted by these cuts. The state is currently working to understand how these cuts will affect state and local cybersecurity efforts and taking steps to keep state and local information systems protected.

The Wisconsin Department of Administration's Division of Enterprise Technology (DET) participated in calls with the Center for Internet Security and other state governments in March and April to learn how these changes will affect Wisconsin. The information below reflects DET's understanding following these calls and is subject to change.

Currently, there is no impact on managed security services. This includes network monitoring for all three branches of state government, local governments, school districts, and libraries; malicious domain blocking and reporting; and intrusion detection functionality for the state. In the last three years, DET has received more than 500 security event notifications due to these services.

### ► How does this affect counties?

Rural and under-resourced counties have relied on free tools and technical assistance through both the MS-ISAC and EI-ISAC to bolster cyber-readiness and improve security practices. Counties also utilize available resources from the MS-ISAC and EI-ISAC to coordinate with other localities, including cities and municipalities, on cybersecurity readiness and information-sharing. Counties support funding assistance for critical cybersecurity tools and resources required to adequately protect county security at all levels, including the cybersecurity of election infrastructures and election workers.

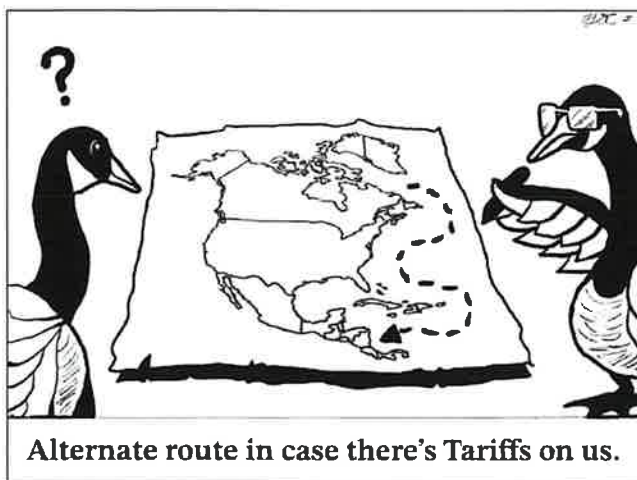
NACo is urging Congress to re-instate federal funding

MS-ISAC has told DET that the following services are or could be impacted by the cuts. The exact impact is currently unknown.

- Cybersecurity advisories and threat intelligence sharing
- Cyber Incident Response Team services, including malicious code analysis, cyber forensics, external vulnerability assessments, and incident response
- Passive threat notification services, including targeted vulnerability notifications, initial access and credential compromise notifications, and IP/domain monitoring
- Cybersecurity awareness, education, and information sharing, including mentoring, working groups, tabletop exercise templates, and webinars
- Cybersecurity assistance services to strengthen cybersecurity for critical infrastructure
- CIS SecureSuite® membership

As much of the Center for Internet Security's and MS-ISAC's remaining funding is also federal, there could be further impacts if additional cuts occur. □


for both initiatives to preserve an information-sharing ecosystem that can support county cybersecurity readiness across critical infrastructure areas and core functions, such as in the administration of the nation's elections. ■



## ENVIRONMENTAL CONSTRUCTION MANAGEMENT

- Turn-Key Renovation & Demolition Services
- Pre-Construction Inspection
- Asbestos & Lead Abatement
- Selective Demolition
- Mechanical Equipment Dismantling





### BALESTRIERI™

AN INDUSTRIAL SERVICE COMPANY • ESTABLISHED 1992

CALL US 262.743.2800  
VISIT OUR WEBSITE [WWW.BALESTRIERIGROUP.COM](http://WWW.BALESTRIERIGROUP.COM)

# The MS-ISAC's Value and Impact Across America

CIS is the home of the Multi-State Information Sharing & Analysis Center (MS-ISAC), the ISAC for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

Recent federal funding cuts to the MS-ISAC have eliminated federal support for some critical cybersecurity services for communities across the country. To prevent SLTT organizations from being vulnerable to cyber attacks, CIS has agreed as an interim measure to continue the services no longer supported by the federal government. However, CIS can only afford to provide this support for a short time. Alternative funding for these critical services with a combination of a membership model for "core" services and a fee for service model for additional services will be required to continue these services going forward.

The MS-ISAC provides low- and no-cost cyber threat information sharing and cyber defense to all 56 states and territories and more than 18,000 public sector organizations that represent American critical infrastructure, including K-12 schools, public hospitals, public water and power utilities, law enforcement, and public transportation.

Over the last 20 years, the MS-ISAC has established itself as a trusted resource in state and local government cybersecurity. The depth of knowledge and experience, as well as the level of collaboration and access to critical information, is something that doesn't exist elsewhere.

## Defending Against Costly Cyber Threats

As threats against SLTTs grow in volume and complexity, the average cost of a cyber attack for state and local governments can range from \$2.83 million to \$9.5 million, with some reports indicating even higher costs, depending on the type and severity of the breach.

Thanks to services provided by the MS-ISAC, there were:

- More than **40,000** potential cyber attacks targeting SLTT networks detected by Albert Network Monitoring intrusion detection sensors and escalated to members by the CIS Security Operations Center (SOC) supporting the MS-ISAC in 2024, with the impacted SLTTs receiving alert notifications in mere minutes, **97% faster** than commercially available alternatives.
- More than **59,000** potential malware and ransomware attacks prevented in 2024 by endpoint protection available to MS-ISAC members through CIS Endpoint Security Services and Endpoint Detection and Response in 2024.
- More than **25 billion** malicious domain connections stopped by our protective DNS service, Malicious Domain Blocking and Reporting (MDBR), in 2024, an average of than **3.3M** blocked requests to known or suspected malicious

*At the request of our valued member organizations, this resource provides a description of the unique value the MS-ISAC provides at an irreplaceable economy of scale to SLTT government organizations nationwide. Members wishing to inform key decision makers about the value of MS-ISAC services you benefit from and the impact of a potential loss of those services can reference the information in this resource.*

## MS-ISAC By the Numbers

As of April 24, 2025

**18,543 members representing:**



domains per member organization in 2024.

- **5.4 million** malicious emails blocked by Email Protection Service in 2024, an average of **77K** per member organization.
- **14 million** web application attacks targeting websites and databases across the U.S. stopped.

The MS-ISAC is committed to helping protect SLTTs and assisting them in defending the critical infrastructure that keeps everyday life moving forward. That infrastructure often includes data-rich and resource poor environments such as school districts, utilities, and transportation systems in towns and cities across the United States. The MS-ISAC released the [Strengthening Critical Infrastructure: SLTT Progress & Priorities report](#) focused on the cybersecurity challenges and priorities unique to state and local governments.

## Providing Critical Services to Protect Critical Infrastructure

Members consistently note the value of no-cost or low-cost services provided by the MS-ISAC such as:

- The support and assistance of the CIS SOC, which is available **24x7x365** to any SLTT or their departments/agencies.
- The MS-ISAC's Cyber Incident Response Team assists many jurisdictions who often lack the staff or resources to combat the complex and increasing volume of cyber threats impacting them.
- The MS-ISAC's protective DNS service, MDBR, supports more than **7,000** SLTTs with a high impact, low maintenance tool that is easy to implement and enables reporting and/or blocking of known malicious domains.
- Nearly **6,500** SLTTs receive and consume actionable cyber threat intelligence focused on and tailored to the SLTT community and curated for delivery into their security incident and event management operational environments.
- An average of **2,400** SLTT representatives attend monthly training and educational webinar sessions.
- More than **2,000** state, local, tribal, and territorial governments take advantage of other technical services, such as the MS-ISAC intrusion detection, endpoint detection and response, email protection, and web application firewall service offerings.

## MS-ISAC By the Numbers

*As of April 9, 2025*

### Top 5 Communities



**K-12 schools  
and districts**  
5,200+ members



**Elections**  
3,800+ members



**Higher Education**  
1,000+ members



**Emergency  
Management, Fire,  
and Law Enforcement**  
800+ members



**Electric Utilities and  
Water and Wastewater  
Sector**  
500+ members



# Impact to Services as a Result of MS-ISAC Cooperative Agreement Reductions

The below chart represents the various services that have previously been or are currently available to MS-ISAC members at no-cost and through cost-effective pricing, arranged according to the impact of federal funding cuts. The subsequent descriptions of each service details the value they provide to MS-ISAC members.

## Services Previously Free with MS-ISAC Membership

Services	Not Impacted by Federal Cuts	Defunded by the Federal Government	Temporarily Continued by CIS	In Process of Service Discontinuation
Albert Network Monitoring and Management (Federally funded)	●			
Annual Meeting		●	●	
CIS Portal	●			
CIS SecureSuite Membership	●			
CIS WorkBench	●			
Communities of Practice		●	●	
Cyber Incident Response Team		●	●	
Cyber Threat Intelligence and Analytical Products		●	●	
Cybersecurity Advisories	●			
Cybersecurity Advisory Services Program (CASP)		●		●
Educational Training Videos		●	●	
Election Day Situation Room		●		●
Election Security Tools and Resources Hub		●	●	
Email Protection Service	●			●
Endpoint Detection and Response (EDR)		●	●	
Foundational Assessment	●			
Leadership Mentoring Program		●	●	
Malicious Domain Blocking and Reporting (MDBR)	●			
Malware IP and Domain List		●	●	
Member Connect	●			
Members-Only Webinars and Forums		●	●	
Nationwide Cybersecurity Review (NCSR)	●			
Onboarding Consultations		●	●	
Passive Threat Notification		●	●	
Post-Incident Vulnerability Scans		●	●	
Quarterly Threat Reports		●	●	
Real-Time Intelligence Feeds		●	●	
Regional Events		●	●	

Services	Not Impacted by Federal Cuts	Defunded by the Federal Government	Temporarily Continued by CIS	In Process of Service Discontinuation
Security Operations Center	●			
Snap Calls		●	●	
Virtual and In-Person Service Reviews		●	●	
Vulnerability Disclosure Program (VDP)		●	●	
Working Groups		●	●	

## Additional MS-ISAC Benefit Options Offered at a Low Fee

Services	Currently Available
Albert Network Monitoring and Management (SLTT funded)	●
CIS CyberMarket	●
CIS Endpoint Security Services (ESS) (SLTT funded)	●
CIS Hardened Images	●
Cyber Liaison Support	●
Malicious Domain Blocking and Reporting Plus (MDBR+)	●
Managed Security Services (MSS)	●
Penetration Testing	●
Vulnerability Assessments	●

## Services Previously Free with MS-ISAC Membership

### Albert Network Monitoring and Management (CA)

Intrusion Detection System (IDS) historically federally-funded through the cooperative agreement (CA) for a subset of members; includes 24x7x365 monitoring by the CIS SOC.

### Annual Meeting

Three-day event bringing together SLTTs across the country to learn, collaborate, and network.

### CIS Portal

Platform that streamlines member support, collaboration with peers, account management, and service management.

### CIS SecureSuite Membership

Provides scalable, customizable tools and resources to guide an

organization's cyber maturity journey. Members can assess endpoint configurations, measure compliance to the CIS Benchmarks, and conduct/track/assess their implementation of the CIS Controls quickly and effectively.

### CIS WorkBench

Community platform used to collaborate with the global cybersecurity community and access CIS SecureSuite resources.

### Communities of Practice

A program that helps better serve the unique needs of the membership and the community of practice in which they work. With the support of member leaders, communities of practice are built to allow members to connect, work on common goals, and push their needs and requirements up to the MS-ISAC Executive Committee and CIS.

### Cyber Incident Response Team

An expert group of cyber first responders, these skilled analysts

walk alongside members during a cybersecurity incident and provide emergency conference calls, forensic analysis, log analysis, mitigation recommendations, reverse engineering, and more.

### Cyber Threat Intelligence and Analytical Products

Reports designed to inform and equip decision-makers to defend against SLTT-focused current and emerging cybersecurity threats, including mitigation recommendations.

### Cybersecurity Advisories

Short, timely notifications containing technical information regarding vulnerabilities in software and hardware or details about a specific cyber incident or threat.

### Cybersecurity Advisory Services Program (CASP)

Provides no-cost, essential, and specialized cyber expertise to help organizations increase cyber maturity,

decrease cyber risks, and make security decisions.

### **Educational Training Videos**

Virtual engagements tailored to meet SLTT-specific needs and interests, featuring peer best practices and exclusive access to industry experts.

### **Election Day Situation Room**

Virtual collaboration space where election offices can coordinate in real time on cyber threats and election security information during an election cycle.

### **Election Security Tools & Resources Hub**

Collection of resources on security best practices developed by a global community of cybersecurity experts that are tailored to the unique nature of election security.

### **Email Protection Service**

Helps detect, prevent, and respond to known and suspected cyber attacks originating via email through inbound mail screening, malware and ransomware protection, phishing protection, spam filtering, and email spoofing protection.

### **Endpoint Detection & Response (EDR)**

Provides election offices with advanced device-level protection to strengthen the cybersecurity of election offices from malicious activity.

### **Foundational Assessment**

Helps evaluate current cybersecurity posture with an assessment aligned with NIST and the CIS Critical Security Controls.

### **Leadership Mentoring Program**

This program has been fostering mentorships for SLTTs for over a decade. It helps build meaningful and mutually beneficial relationships through peer-to-peer connection while promoting the increased maturity of leaders and security programs across the SLTT community.

### **Malicious Domain Blocking & Reporting (MDBR)**

Easy-to-configure protective DNS service that is highly-effective at

proactively blocking network requests from known harmful web domains.

### **Malware IP & Domain List**

Weekly report with identified malicious IP addresses and domains observed targeting SLTT networks.

### **Member Connect**

Online forum that allows members to collaborate, share ideas, ask questions, and exchange valuable resources with fellow members in real-time.

### **Members-Only Webinars & Forums**

Monthly, bimonthly, and ad-hoc webinars focus on special topics, incidents, and the State of the ISACs to increase cyber awareness and education as well as forums designed to information and best practices on certain topics of interest (e.g., Whole of State/SLCGP Forum).

### **Nationwide Cybersecurity Review (NCSR)**

No-cost, anonymous annual self-assessment designed to measure gaps and capabilities of organizations' cybersecurity programs and develop benchmarks for year-to-year cybersecurity improvements, as requested by the Senate Appropriations Committee.

### **Onboarding Consultations**

Personalized 1:1 call within the first 90 days of enrolling helping guide members with a personalized road map for improving cybersecurity and assistance with the adoption of our low cost and no cost resources.

### **Passive Threat Notification**

Provides constant monitoring and notification for malicious activity related to member IP/domains on the dark web and criminal forums; also performs scans of member internet-facing architecture for emerging critical vulnerabilities.

### **Post-Incident Vulnerability Scans**

A service that assists members who have experienced cyber incidents with assessments to verify their remediation efforts.

### **Quarterly Threat Reports**

Analyzes quarterly SLTT-focused cyber threat intelligence (CTI) trends and provides threat forecasting based on MS-ISAC internal and opensource reporting.

### **Real-Time Intelligence Feeds**

Real-time cyber threat intelligence feeds available in multiple formats with simple authentication; over 6,000 SLTT subscribers.

### **Regional Events**

One or two day in-person events hosted around the country, designed to unite members around relevant cybersecurity topics. These events emphasize networking, addressing member challenges and requirements, fostering collaboration, and developing a strong sense of community.

### **Security Operations Center**

24x7x365 security operations center and analysis unit that functions like an extension of MS-ISAC member's security team to monitor, analyze, and respond to cyber incidents.

### **Snap Calls**

Short-notice, community calls to address concerns with emerging threats or vulnerabilities; examples include calls for Log4j, SolarWinds, and the recent CrowdStrike global outage.

### **Virtual and In-Person Service Reviews**

Customized sessions to help members identify necessary services to improve cybersecurity maturity.

### **Vulnerability Disclosure Program (VDP)**

Formal program to receive, validate, remediate, and communicate vulnerability data on specific technology systems from external security researchers; gives permission to security researchers to ethically find and report vulnerabilities in an organization's public-facing systems such as websites and voter registration databases.

### **Working Groups**

Focused committees working to share

ideas, generate recommendations, and produce deliverables to support the MS-ISAC and member-related programs.

## **Additional MS-ISAC Benefit Options Offered at a Low Fee**

### **Albert Network Monitoring and Management (SLTT funded)**

Cost-effective, custom-built Intrusion Detection System (IDS) for SLTTs, critical infrastructure, and public education entities with industry-leading threat notification times that saves time and money by reducing an average of 75% of false positive alerts common to IDS solutions.

### **CIS CyberMarket**

The only cybersecurity marketplace specifically designed for U.S. SLTTs to find cost-effective cybersecurity services and solutions vetted by experts and tailored to their unique needs.

### **CIS Endpoint Security Services (ESS) (SLTT funded)**

Device-level protection that provides active defense against both known (signature-based) and unknown (behavioral-based) malicious activity as well as effective defense against encrypted malicious traffic.

### **CIS Hardened Images**

Virtual machine images pre-configured to the CIS Benchmark recommendations that help organizations implement built-in security in their cloud environments.

### **Cyber Liaison Support**

CIS maintains Liaison Analysts within CISA Threat Hunt to assist in brokering priority efforts between the SLTT/Elections communities and the federal government.

### **Malicious Domain Blocking & Reporting Plus (MDBR+)**

MDBR with additional host-level granularity and control; provides real-

time reports, custom configurations, and off-network device protection to reduce risk

### **Managed Security Service (MSS)**

Round-the-clock expert security log monitoring that identifies signs of malicious or suspicious activity and alerts on potential threats.

### **Penetration Testing**

Helps organizations prepare for real-world cyber attacks through simulations that safely review the security posture of their web applications and networking devices.

### **Vulnerability Assessments**

Helps identify vulnerabilities in networks and web applications so members can take appropriate remediation steps to improve their security posture.

## **Share Your MS-ISAC Value and Impact Story**

Reach out to the MS-ISAC team at [info@cisecurity.org](mailto:info@cisecurity.org) with the subject line 'My MS-ISAC Story' so that we can leverage your anonymized success stories as we communicate the importance of the MS-ISAC to the SLTT community.

**Ruetten, Jennifer**

---

**From:** MS-ISAC <noreply@msisac.org>  
**Sent:** Wednesday, October 1, 2025 9:36 AM  
**Subject:** MS-ISAC Update — Funding and Our Future as a Member-Driven Community

Dear Members,

The Center for Internet Security (CIS) has been informed that the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) have chosen not to renew federal funding that has supported the MS-ISAC for the past 20 years. In a recent press release, CISA also announced this and indicated that “[CISA Strengthens Commitment to SLTT Governments](#)”. The press release also highlights offerings CISA has provided, which should not be seen as replacements for — or in competition with — the broad, scalable, and highly-valued products and services offered by the MS-ISAC.

While we are disappointed by DHS/CISA’s decision, CIS and your MS-ISAC Executive Committee has been preparing for this possibility, and the MS-ISAC is well-positioned to move forward. To ensure continuity of service, the MS-ISAC will now fully transition to the fee-based membership model previously communicated. This model enables us to continue delivering high-impact cybersecurity services, including multidimensional threat intelligence, executive-level products, best practices, collaboration opportunities, and support for “whole of state” initiatives.

Also, as a result of the loss of federal funding, membership tier pricing will be adjusted to reflect the “no Cooperative Agreement/Federal Funding” structure previously shared. However, as previously agreed, organizations that had enrolled under the Single Organization membership prior to September 1 are grandfathered in at their original purchase price for a period of 18 months.

As a program within the nonprofit and nonpartisan Center for Internet Security, the MS-ISAC remains deeply committed to serving the state, local, tribal, and territorial (SLTT) community and strengthening the collective cybersecurity resilience we’ve developed together. We understand the challenges that states, territories, and local organizations are facing as we jointly proceed with this transition to a fee-based membership. Our promise is that we will continue to make every effort to support those members who are engaged with us in pursuing membership under one of the fee-based options. If you have questions or need assistance, please reach out to [info@cisecurity.org](mailto:info@cisecurity.org).

The security challenges that you face continue to increase. Our joint objective is to provide you with cost-effective support to help you meet these challenges.

Best regards,

Multi-State Information Sharing and Analysis Center (MS-ISAC)

24x7 Security Operation Center  
[SOC@cisecurity.org](mailto:SOC@cisecurity.org) 1-866-787-4722





# MS-ISAC Single Organization Membership

## Sustainable Cybersecurity Tailored for SLTTs

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) funding model ensures long-term support for the vital cybersecurity services your organization depends on, strengthening the U.S. State, Local, Tribal, and Territorial (SLTT) community nationwide.

## A Trusted Partnership to Protect Your Community

With SLTTs on the front lines of defending the nation against pervasive cyber attacks, you need a partner you can trust. Powered by the 24x7x365 CIS Security Operations Center, the MS-ISAC delivers real-time threat intelligence and response to support SLTTs without round-the-clock security teams.

## For SLTTs, by SLTTs

MS-ISAC membership means joining a collaborative defense network. You gain exclusive access to essential tools and information while contributing to the security of others. Whether you're a large agency or a small township, there's a membership tier tailored to your needs and budget.

## Benefits Provided with MS-ISAC Membership

### Threat Intelligence and Distribution

- SLTT Specific Threat Intelligence Analysis Products and Reporting
- MS-ISAC Threat Intelligence Platform STIX/TAXII and MISP Access
- Virtual Threat Intelligence Briefings (SLTT threat brief)

### Member Collaboration and Engagement

- Exclusive access to a collaborative peer community
- 1:1 service consultations with CIS cybersecurity experts
- MS-ISAC Annual Membership Meeting
- Monthly membership calls
- Best practice webinars led by experienced peers and top experts
- SLTT mentorship program

\*Member benefit currently funded by the federal government.

### Incident Response & Forensic Services

- MS-ISAC Incident Response & Forensic Services (as resources allow)

### Security Operations Center (SOC)\*

- 24x7x365 SOC Access
- SOC Alerts, Advisories, Weekly Malicious IP/Domain List
- Passive Threat Notification Service
  - Targeted Vulnerability Notifications
  - Initial Access Broker (IAB) Monitoring
  - Breached Credential Monitoring
  - IP and Domain Monitoring

### Services and Programs\*

- Malicious Domain Blocking and Reporting (MDBR)
- Annual cybersecurity self-assessment (NCSR)

## MS-ISAC Annual Membership Pricing - Single Organization

Pricing tiers are based on total annual operating budget of the organization you intend to cover with your Single Organization Membership. All benefits of MS-ISAC membership are available to all members across all tiers.

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Entity Annual Operating Budget	<\$25M	\$25M – \$100M	\$100M – \$250M	\$250M – \$1B	>\$1B
Current Pricing†	\$995	\$1,995	\$4,995	\$9,995	\$17,500
Pricing if No Federal Funding††	\$1,495	\$3,495	\$9,995	\$17,995	\$29,995

†Based on existing federal funding levels, currently set to expire September 30, 2025.

††Pricing if the current federal funding is not renewed for FY 2026.

## Optional, Cost-Effective Add-On Services

- Albert Network Monitoring and Management
  - Network intrusion detection system custom built for SLTTs
- Malicious Domain Blocking and Reporting Plus (MDBR+)
  - Protective DNS service with custom configurations and real-time reporting
- CIS Managed Detection and Response™ (CIS MDR™) (Formerly referred to as Endpoint Security Services (ESS))
  - Device-level protection for endpoint devices including workstations and servers
- Managed Security Services (MSS)
  - Round-the-clock expert security log monitoring
- Red Team Services
  - Vulnerability Scanning, Penetration Testing
- Virtual or In-Person Delivery of Customized Tabletop Exercise (TTX) - Coming Soon
- Virtual Threat Intelligence Briefings (Customized for Member) - Coming Soon
- Malicious Code Analysis Platform (MCAP) Access - Coming Soon

