Multi-State Information Sharing & Analysis Center™

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort designated by The Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's State, Local, Tribal and Territorial governments.

Multi-State Information Sharing and Analysis Center
31 Tech Valley Drive
East Greenbush, NY 12061
info@msisac.org
soc@msisac.org
518-266-3460

Table of Contents:

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

What We Offer

The MS-ISAC provides ***real-time network monitoring***, threat analysis, and early warning notifications through our 24x7 cybersecurity operations center.

The U.S. Department of Homeland Security has designated the MS-ISAC as its ***key cybersecurity resource*** for State, Local, Tribal and Territorial governments, including chief information security officers, homeland security advisors and fusion centers.

We perform ***incident response and remediation*** through our team of security experts.

The MS-ISAC conducts ***training sessions and webinars*** across a broad array of cybersecurity related topics.

We continually develop and distribute ***strategic, tactical and operational intelligence*** to provide timely, actionable information to our members.

We provide ***cybersecurity resources*** for the public, including daily tips, monthly newsletters, guides and more.

Who We Serve

CISOs, CIOs, and other security professionals from:

- U.S. State, Local, Tribal and Territorial Governments
- U.S. State/Territory Homeland Security Advisors
- State and Local Government Fusion Centers and Local Law Enforcement Entities

How We Do Business

- We cultivate a c***ollaborative environment*** for information sharing.
- We focus on ***readiness and response***, especially where the cyber and physical domains meet.
- We facilitate ***partnerships*** between the public and private sectors.
- We focus on ***excellence to*** develop industry leading, cost- effective cybersecurity resources.
- ***Collectively we achieve much more*** than we can individually.

"All services performed by the MS-ISAC were not only prompt, but professional and efficient. Communication was handled very well, and the report was fantastic."
- MS-ISAC Member

MS-ISAC Membership Overview

The Multi-State Information Sharing and Analysis Center (MS-ISAC), is part of the nonprofit Center for Internet Security (CIS). The MS-ISAC is a voluntary community focused on improving cybersecurity for State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC started in 2003. Since then, we have built and nurtured an environment of collaboration and information sharing. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for State, Local Tribal and Territorial governments, including chief information security officers, homeland security advisors and fusion centers.

There is **no cost to join the MS-ISAC**, and **membership is open to all SLTT government entities**. The only requirement is the completion of a membership agreement, which outlines member's responsibilities to protect information that is shared.

MS-ISAC Member Responsibilities

In order to maintain the MS-ISAC's trusted, collaborative environment, each member understands that the following principles of conduct will guide their actions, and each member agrees to:

- share appropriate information between and among the members to the greatest extent possible;
- recognize the sensitivity and confidentiality of the information shared and received;
- take all necessary steps to protect confidential information;
- transmit sensitive data to other members only through the use of agreed-upon secure methods; and
- take all appropriate steps to help protect our critical infrastructure.

Members are also asked to share their **public-facing IP ranges** and **domain space** with the MS-ISAC to facilitate efficient and effective discovery and notification of system compromises.

"We so appreciate all that you have done to help! I can't tell you how much it helped to know that you were with us through this (incident)."
- MS-ISAC Member

"I can honestly say that your organization has made an immediate impact in our overall security readiness. Thank you." - MS-ISAC Member

The MS-ISAC Security Operations Center

What is the MS-ISAC SOC?

The MS-ISAC operates the Security Operations Center (SOC), a 24x7 joint security operations and analytical unit that monitors, analyzes and responds to cyber incidents targeting U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

Core Services of the MS-ISAC SOC:

The SOC provides real-time network monitoring, early cyber threat warnings and advisories, and vulnerability identification and mitigation.

The MS-ISAC SOC:

- **Cyber Vulnerability & Threat Research**: Analysts monitor federal government, third parties, and open sources to identify, analyze and then distribute pertinent information.
- **Compromised System Notifications**: provided to members in the event of a potential compromise identified based on the MS-ISAC's unique awareness of the threat landscape.
- **Cyber Security Exercises**: The MS-ISAC participates in federally sponsored cyber security exercises and acts as a voice for SLTT governments in planning meetings.
- **Fee Based Services**: The MS-ISAC offers a variety of fee based services for SLTT government entities to take advantage of. (See pages 18-19)
- **Monitoring Services**: We currently provide monitoring services for 60+ SLTT government entities through a variety of security devices. (See pages 8 & 18)
- **Soltra Edge**: Soltra Edge is a platform that utilizes STIX and TAXII in order to automate cybersecurity threat intelligence sharing. Leveraging these standards enables users to send and receive threat information from machine to machine. We currently maintain an Internet facing instance of Soltra Edge available to our MS-ISAC members.

Additional Services Include:

The Computer Emergency Response Team (**CERT)** provides malware analysis, computer and network forensics, malicious code analysis and mitigation recommendations.

The **Intel** Analysis unit takes known information about situations and entities and makes forward-leaning assessments regarding the cyber trends, actors, tactics, techniques, and procedures (TTPs).

The **Partner Liaison** group includes MS-ISAC employees located at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C. and the National Cyber Investigative Joint Task Force (NCIJTF). We also incorporate representatives from DHS, U.S. Secret Service (USSS), Homeland Security Investigations (HSI), Federal Bureau of Investigation (FBI), New York State Intelligence Center (NYSIC), and the New York Power Authority (NYPA) at the MS-ISAC headquarters in New York.

"We appreciated the time the MS-ISAC CERT provided to us to validate our findings and provide valuable insight on opportunities for future improvement. The states are very blessed to have access to the talents of the MS-ISAC CERT in times of crisis." - MS-ISAC Member

Reporting an Incident and Requesting Assistance

Members are encouraged to report incidents, even if they are not requesting direct assistance, to improve situational awareness to benefit all members. Types of incidents to report include the following:

- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Compromised password(s)
- Execution of malware, such as viruses, trojans, worms or botnet activity
- Defacement of a government web page
- Disruption or attempted denial of service (DoS)
- Unauthorized access to information
- Unauthorized use of a system for transmitting, processing or storing data
- Unauthorized use of system privileges

To report an incident, please contact the MS-ISAC SOC for 24x7 assistance:

Phone: 1-866-787-4722
Email: soc@msisac.org

If the incident you are reporting does require direct assistance, the Computer Emergency Response Team (CERT), a unit comprised of highly trained staff, are able to assist you with a cybersecurity incident at no cost.

Our incident response experts can assist with the following:

- Emergency conference calls
- Forensic analysis
- Log analysis
- Mitigation recommendations
- Reverse engineering
- Verbal report 24 hours following the reported incident
- Written report 1 week following the close of the incident

"I will continue to leverage this expert and valuable service as long as it exists. The MS-ISAC CERT was once again very efficient and provided a robust root cause analysis in a timely fashion." - MS-ISAC Member

"Thank you for providing this invaluable service!"
- MS-ISAC Member

Network Monitoring and Analysis Services

The MS-ISAC offers a network monitoring service known as Albert. Albert is based on the U.S. DHS Einstein technology, which was designed to generate and collect network flows (netflows). The MS-ISAC has enhanced this technology to include behavioral and signature-based detection methods, as well as historical analysis capabilities.

The Albert service consists of a sensor(s) placed on an organization's network—typically outside the perimeter firewall and Internet connection—that collects network data and sends it to the MS-ISAC for analysis. Based on the MS-ISAC's vast repository of indicators of compromise, we are able to identify malicious activity and alert the organization.

This service is committed to building and maintaining the most comprehensive set of detection rules and signatures impacting SLTT entities.

Why is the Albert Service Unique?

- Government-specific focus and tailored to SLTT government's cybersecurity needs
- Correlation of data from multiple public and private partners;
    - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties
    - When a major new threat is identified, the MS-ISAC will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTT's, including nation-state attacks.
- MS-ISAC staff are deployed at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C. and the National Cyber Investigative Joint Task Force (NCIJTF). This staffing structure facilitates valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Experienced cybersecurity analysts review each cybersecurity event, which results in minimizing the number of false-positive notifications. This system allows first responders to focus on actionable events.
- Availability of an Incident Response Team for forensic and malware analysis which is part of the no cost MS-ISAC membership.
- Cost effective solution that is significantly less expensive than the purchase and maintenance of a typical commercial IDS/IPS solution. (See Page 18)

In addition to the Albert monitoring service, we also have the ability to monitor traditional network security devices such as firewalls, IDS/IPS, web proxies, and host based intrusion detection devices. This monitoring is accomplished with our Managed Security Services (MSS) offering. All events generated by MSS are evaluated by our SOC analysts and escalated to the affected entity. (See Page 18)

Malicious Code Analysis Platform

The Malicious Code Analysis Platform (MCAP) is a web-based service that enables members to submit and analyze suspicious files, including executables, dlls, documents, quarantine files and archives, in a controlled and non-public fashion. Additionally, the platform enables users to perform threat analysis based on domain, IP address, URL, HASH, and various IOCs.

This platform allows users to obtain the results from analysis, behavioral characteristics and additional detailed information that enables them 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.

This platform is available to all members free of charge. To register for an account, send an email to mcap@cisecurity.org using the following format:

Subject Line: "MCAP - Account Request"
Body for the Email:

- First Name
- Last Name
- Name of State, Local, Tribal or Territorial government entity
- Email Address (must be affiliated with MS-ISAC member)

Vulnerability Management Program

The Vulnerability Management Program alerts our membership, on a monthly basis, regarding out of date software that could potentially be a threat to your assets. A scripted GET request is sent to each of the over 24,000 SLTT domains we maintain to pull data on versioning information related to a given domain.

What Data Are We Collecting?

- Server Type and Version (IIS,Apache, Nginx, etc.)
- Web Programming Language and Version (PHP, ASP, etc.)
- 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.

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.

For questions regarding the domains that the MS-ISAC has on file for your organization, please contact info@msisac.org. Domain listings can be edited at any point in time during your membership.

Cyber Threat Informational & Analytical Products

- **Cyber Advisories:** Cyber Advisories are short and timely emails containing technical information regarding vulnerabilities in software.
- **Cyber Alerts:** Cyber Alerts are extremely short and timely non-technical emails containing information on a specific cyber incident or threat.
- **Cyber Intel Advisory:** Cyber Intel Advisories provide detailed information and warning notices with limited analysis. Recipients are invited to attach their own seals/shields and republish the document as a joint shield paper.
- **Cyber Threat Briefings:** The MS-ISAC SOC provides cyber threat briefings based on our expertise of the cyber threat landscape and incidents targeting SLTT governments.
- **Desk References:** Desk references provide in-depth information and intelligence analysis on specific topics, such as active hacktivist groups and the most common malware, frauds and scams.
- **Intel Byte:** Intel Bytes are a brief analytical summary on timely local or world events or significant threats, and provide analytical intelligence.
- **Intel Paper:** Intel Papers provide in-depth analysis and detailed information regarding the background, history, tools, techniques, and/or procedures on a particular topic. They provide our members with a deeper level of understanding.
- **Joint Paper:** The MS-ISAC coordinates with federal and SLTT governments, fusion centers and other agencies to produce joint analytical papers on a variety of topics.
- **Monthly Cyber Update:** The Monthly Cyber Update is a newsletter produced for the National Governors Association Governors Homeland Security Advisory Council that summarizes and provides analysis on recent news articles. Members may attach their own seals/shields and redistribute the newsletter as a joint shield paper.
- **Security Primers:** Security Primers are a one-page summary that recommend the best response to a specific scenario. The Primers increase security awareness and encourage secure behavior.
- **Seminars:** MS-ISAC Seminars are monthly meetings that provide training on a variety of topics. Continuing Professional Education (CPE) credit is available upon request.
- **Situational Awareness Report (SAR):** These highlight the MS-ISAC's previous month's activities and statistics related to incident response, network monitoring and general information gathering.
- **White Papers:** The SOC produces white papers to explain technical topics of interest to members and partners.

"It was very helpful to have the MS-ISAC to turn to at this difficult time. They were extremely helpful every step of the project." - MS-ISAC Member

MS-ISAC Member Initiatives & Collaborative Resources

MS-ISAC membership enables entities to participate with their peers across the country, sharing knowledge, building relationships, and improving cybersecurity readiness and response.

- **Annual In-Person Meeting:** Each year, the MS-ISAC hosts an annual multi-day event bringing all members together, along with the federal government and other partners. We focus on action-oriented deliverables that are most important to the members. The meeting is open to all MS-ISAC members interested in attending. There is no registration fee for this event.
- **Emergency conference calls:** Members have access to conference calls to brief all members on major incidents or emerging events
- **ESP Tool:** The CIS Enumeration and Scanning Program (CIS-ESP) is an application built to be deployed in an enterprise Windows environment to assist in the collection of data to determine if a compromise has occurred. The information collected will help understand the scope of an incident and identify active host-based threats on a computer network. The application works by enumerating and polling systems within an Active Directory environment by way of Windows Management Instruction (VMI) queries. This process is used entirely for data collection and no modifications are made to the systems being scanned.
- **Members-Only Secure Portal:** The MS-ISAC has a compartment on the US-CERT portal which allows our membership a secure and confidential platform for sharing information. The portal includes the MS-ISAC cyber alert level map—a visual representation of current cyber status of each state, updated on a monthly basis; library of policies, guides, recorded webcasts, and many additional member resources.
- **Monthly Threat Briefing:** one-hour webcast briefings that provide members with updates on the threat landscape, status of national initiatives impacting them, relevant news from members; DHS has a standing agenda item on each call
- **Monthly Vendor Patch Release Calls:** technical discussions regarding patches and updates
- **Security Benchmarks:** Consensus-based security configuration PDF guides that help to improve your cyber security posture
- **Security Benchmarks Membership:** MS-ISAC members can receive discounts between 30-50% off of Security Benchmarks Membership, leveraging over 100 configuration benchmarks covering over 14 technology groups, and can use CIS-CAT to assess an unlimited number of assets for a single upfront cost.
    - **CIS-CAT:** MS-ISAC members have access to a free 30-day trial of CIS-CAT, a Configuration Assessment Tool, containing 60+ CIS Benchmarks (See Pages 13 & 19)
- **Special Pricing for Cyber Security Training and Solutions:** specially negotiated pricing for SLTT governments on the most in-demand training courses and security products offered by industry leaders (See Page 19)
- **Workgroups:** focused working committees to share ideas, generate recommendations and produce deliverables to support the MS-ISAC and member-related programs (See Page 14)

MS-ISAC Workgroups

These workgroups are voluntary committees focused on specific initiatives and deliverables in support of the MS-ISAC mission.

Who can participate in a workgroup?

Any member from:

- State, Local, Tribal and Territorial (SLTT) governmental agencies
- Fusion Center personnel
- Homeland Security Advisors
- Law Enforcement
- Federal government

What do the workgroups do?

They serve a significant role in the creation and implementation of MS-ISAC initiatives. These workgroups are also a tremendous opportunity to collaborate with your peers across the country. These groups identify current issues facing SLTT governments and help determine the future course of addressing cybersecurity challenges. They have been responsible for:

- authoring the *Nationwide Cyber Security Review* question set and analyzing the results;
- participating in the development and execution of cyber security exercises;
- increasing participation in National Cyber Security Awareness Month activities;
- working with the federal government to provide free training to members; and
- creating important membership materials.

How much time will I need to commit?

- Level of commitment varies by group.
- Groups generally meet by phone monthly and in person annually.
- Extent of involvement is completely your choice.

How do I join a workgroup?

Send an email to info@msisac.org, with "Workgroup Request" in the subject line, and include the following:

- Name
- Workgroup of interest
- Entity/Agency Name
- Email and telephone number

Share your expertise by joining a Workgroup today!

Current Workgroups:

Business Continuity, Recovery, and Cyber Exercise

Co-Chairs: Andrew Dolan, Jeremy Mio, Lynne Pizzini

Focuses on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations and communications.

Cyber Security Metrics

Co-Chairs: Gary Coverdale, Karen Sorady

Focuses on recommending and implementing methodologies to help SLTT entities with cyber security metrics and compliance inventory, assessment and audit of their cyber security assets. This workgroup works jointly with DHS, NASCIO and NACo to support the DHS Nationwide Cyber Security Review.

Education and Awareness

Co-Chairs: Eugene Kipniss, Danielle Cox, Kelly Stegmann, Michael McCray, Ralph Johnson

Focuses on implementing innovative strategies, improving existing programs, and promoting successful localized initiatives for national cybersecurity education, awareness, and training content to support the overall mission of MS-ISAC.

Industrial Control Systems (ICS)

Co-Chairs: Ben Spear, Mike Lettman, Tim Guerriero

Focuses on providing a vehicle for MS-ISAC members to increase their knowledge and awareness of threats, vulnerabilities, and mitigation strategies impacting the ICS cyber infrastructure.

Intel and Analysis

Co-Chairs: Arnold Kishi, Stacey Wright, Walter Tong

Focuses on promoting the development, understanding, and awareness of actionable intelligence and analysis.

Legislative and Compliance

Co-Chairs: Chris Buse, Erin Dayton, Vince Simonowicz

Focuses on tracking all national, major legislation, rules and regulations relating to cybersecurity issues.

Mentoring Program

Co-Chairs: Gary Coverdale, Jay White, Jessica Williams, Mike Aliperti, Theresa Masse

Focuses on pairing new security leaders in management positions (such as Chief Information Security Officers and Chief Security Officers) with more experienced security leaders to enhance their skillsets and foster personal and professional growth.

Nationwide Cyber Security Review

The Nationwide Cyber Security Review (NCSR) is a voluntary self-assessment survey to evaluate cybersecurity management.

The Senate Appropriations Committee has requested an ongoing effort to chart nationwide progress in cybersecurity and identify emerging areas of concern. In response, the U.S. Department of Homeland Security (DHS) has partnered with the MS-ISAC, the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop and conduct the NCSR.

Who can participate?

All States (and agencies), Local governments (and departments), Tribal and Territorial governments.

Advantages of Participation:

- free and voluntary self-assessment to evaluate your cybersecurity posture;
- customized reports to help you understand your cybersecurity maturity, including:
  - a detailed report of your responses along with recommendations to improve your organization's cybersecurity posture;
  - additional summary reports that gauge your cybersecurity measures against peers (using anonymized data); and
  - to prioritize your effort to develop security controls.
- benchmark to gauge your own year-to-year progress;
- metrics to assist in cybersecurity investment justifications; and
- contribute to the nation's cyber risk assessment process.

How does the Nationwide Cyber Security Review work?

- hosted on a secure portal
- based on the NIST Framework
- based on key milestone activities for information risk management
- closely aligned with security governance processes and maturity indexes embodied in accepted standards and best practices
- covers the core components of cybersecurity and privacy programs
- designed to be completed in about an hour

When does the survey take place?

The annual survey will be available October 1, to coincide with National CyberSecurity Awareness Month. Participants must submit their results by November 30.

For more information, and to register, visit:
http://msisac.cisecurity.org/resources/ncsr

Survey

The NCSR provides survey participants with instructions and guidance. Additional support is available including, supplemental documentation and the ability to contact the NCSR helpdesk directly from the survey.

Once the NSCR is complete, participants will have immediate access to an individualized report measuring the level of adoption of security controls within their organization. This report includes recommendations on how to raise your organization's risk awareness. In alternate years only (odd numbered years), the MS-ISAC and DHS will aggregate all review data and share a high level summary with all participants. The names of participants and their organizations will not be identified in this report. This report is provided to Congress in alternate years (odd numbered years) to highlight cyber security gaps and capabilities among our State, Local, Territorial and Tribal Governments.

Partners

The U.S. Department of Homeland Security (DHS) has partnered with the MS-ISAC, the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop the Nationwide Cyber Security Review.

DHS is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. National Protection & Programs Directorate leads DHS's efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy. Founded in 1969, the National Association of State Chief Information Officers (NASCIO) is a nonprofit, 501(c)3 association representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. The primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as associate members. Representatives from federal, municipal, international government and non-profit organizations may also participate as members. Private-sector firms join as corporate members and participate in the Corporate Leadership Council.

The **National Association of Counties (NACo)** is the only national organization that represents county governments in the United States. Founded in 1935, NACo provides essential services to the nation's 3,069 counties. NACo advances issues with a unified voice before the federal government, improves the public's understanding of county government, assists counties in finding and sharing innovative solutions through education and research, and provides value-added services to save counties and taxpayers money. For more information about NACo, visit www.naco.org.

Cybersecurity Education

We promote proactive education of cybersecurity. The MS-ISAC produces numerous communications to engage our members and help national efforts for better cybersecurity.

Education and Awareness Materials

- **Daily Cyber Tips**
- **Monthly Newsletters**: These newsletters use non-technical language, and they can be rebranded to suit individual member's needs. Newsletter topics include details on the most current threats and suggested best cybersecurity practices.
- **Bi-Monthly National Webcasts**: feature timely topics and experts from the public and private sector sharing insight on addressing cyber challenges.

Cyber Security Toolkit

This Cyber Security Toolkit features educational materials designed to raise cyber security awareness. Digital and hard copy materials are distributed to members. Members are encouraged to brand for their own organizations.

Best of the Web Contest

The MS-ISAC conducts an annual Best of the Web contest to recognize state and local governments who use their websites to promote cybersecurity. We review these cybersecurity websites for all 50 state governments and many local governments. The judging is based upon several criteria including cyber security content, usability, accessibility, and appearance.

The contest recognizes outstanding websites and highlights them as examples for others to consider when they are developing or re-designing their own sites. One overall winning website will be chosen in the state/territory category and one will be chosen in the local government category.

The Best of the Web Contest kicks off in beginning of October which is Cyber Security Awareness Month. The winners are announced at the end of the month.

Poster Contest

The MS-ISAC conducts an annual national K-12 Computer Safety Contest to encourage young people to use the Internet safely. The contest encourages young people to create cybersecurity messages other kids will appreciate and apply to their own lives.

The contest is open to all public, private or home-schooled students in kindergarten through twelfth grade. Winning entries of the National Poster Contest are what make up the next year's MS-ISAC Calendar, which is distributed to every MS-ISAC member.

The MS-ISAC Poster Contest is launched at the beginning of Cyber Security Awareness Month. Submissions are due the following January.

For questions regarding education and awareness materials or participation in any of the items listed above, please contact info@msisac.org.

Security Benchmarks Membership

CIS is a leader in the development and distribution of consensus-based, internationally recognized best practices for assessing and improving cybersecurity for private industry, government and academia. CIS secure configuration benchmarks and automated assessment tools are used by hundreds of organizations worldwide and are accepted for compliance with many industry standards, including FISMA, PCI, and HIPAA.

CIS Security Benchmarks members can leverage more than 100 CIS configuration benchmarks covering over 14 technology groups. These members can also use CIS-CAT to assess an unlimited number of assets for a single, upfront fixed cost.

How can CIS Benchmarks Membership and the member only resources benefit my organization?

CIS offers affordable, industry-recognized solutions to help your organization save time and money by providing resources that:

- Rapidly identify security vulnerabilities
- Measure security performance against industry best practices
- Satisfy compliance obligations http://benchmarks.cisecurity.org/compliance
- Improve internal security policies and procedures by leveraging best-practice guidance
- Assess a system(s) compliance with security requirements by using the CIS Configuration Assessment Tool (CIS-CAT)
- Quickly implement benchmark guidance by using CIS remediation resources
- Measure and report compliance over time per device, technology, or overall

What are the benefits of Security Benchmarks membership?

- The right to distribute the Security Benchmarks resources within your organization
- Access to CIS-CAT (See Page 19)
- Access to the member only resources on the CIS Community Website, including:
  - Word/Excel versions of Benchmarks
  - Benchmarks in XML/XCCDF/OVAL format which facilitates automated configuration assessment
  - Automated remediation content (i.e., Group Policy Objects)
  - CIS Hardened Virtual Images through Amazon Web Services (AWS)
  - Tutorials and webcasts
  - Member only discussion areas
- Timely electronic notification of new and updated resources
- Enhanced support from staff and developers
- Visibility of your organization's commitment to Internet security through its inclusion on the CIS member list http://benchmarks.cisecurity.org/members
- Use of the CIS Security Benchmarks Membership Mark on your organization's website and documents

For a complete list of benefits, see http://benchmarks.cisecurity.org/membership

Free trial of CIS-CAT

A 14-day trial of CIS-CAT is available to companies considering membership. To start your trial today, visit https://benchmarks.cisecurity.org/freetrial

Fee Based Services for SLTT Entities

Network Monitoring and Analysis Service (Albert) is a near real-time, 24x7 network monitoring and analysis service that identifies and alerts on traditional and advanced threats within an enterprise network. Pricing based on Average Internet Utilization Size. One time initiation fee of $900 applies.

- Size Up to 10mb/sec - $620/Month
- Size >10mb/sec – 100mb/sec - $940/Month
- Size >100mb/sec- $1,460/Month

Managed Security Services (MSS) is comprised of monitoring and/or management of security devices:

- Security Event Analysis & Notifications 24x7
- Monitoring and Management services are available for the following security devices.
    - Firewall monitoring
    - Host-based Intrusion Detection System monitoring
    - IDS/IPS monitoring and management
    - Proxy monitoring

Vulnerability Assessment Services can identify, prioritize and report critical vulnerabilities with MS-ISAC network and web application assessments.

- Network Assessment
- Web Application Assessment, including manual analysis of reported vulnerabilities
- Prioritization of vulnerability remediation
- Customized reporting & vulnerability remediation support included
- Payment Card Industry (PCI) compliance scanning available
- Scheduled (Monthly, Quarterly, Yearly)

Web Application Assessment	Annual Cost per Web App Scanned		
	One Time Assessment	Quarterly Assessments	Monthly Assessments
1st Web App per Entity	$1,025	$1,322	$1,918
Additional Web App per Entity	$569	$867	$1,463

Network Assessment	Annual Cost per *Live* IP Scanned		
Service Level Based on the Number of Live IPs Scanned per period per Reporting Entity	One Time Assessment	Quarterly Assessments	Monthly Assessments
10	$88	$120	$189
16-25	$67	$92	$151
26-50	$55	$75	$128
51-100	$44	$59	$105
101-200	$26	$38	$77
201-500	$22	$32	$65
501-2,000	$19	$27	$53

MS-ISAC Consulting Services (Statement of Work Required) for the following items:

- Social Engineering (Phishing Exercises)
- External Network Penetration Testing
- Web Application Penetration
- Comprehensive Security Review

Security Benchmarks Membership allows the government entity the right to use and distribute the Security Benchmarks resources throughout their organizations to secure *internal* systems only. Membership fees are based on the total number of people employed at an organization. A detailed agency list is required at time of membership quote and/or enrollment. The annual fee and multi-year discount option schedule for SLTT governments is below. Contact us at info@msisac.org for more information.

Security Benchmarks Membership

Organization Employee Range	1-Year Membership Cost (30% Savings)	2-Year Membership Cost (30% Savings)	3-Year Membership Cost (30% Savings)
250,000 or more	$9,926	$ 19,852	$ 29,778
100,000 to 249,999	$9,191	$ 18,382	$ 27,573
50,000 to 99,999	$8,456	$ 16,912	$ 25,368
25,000 to 49,999	$7,721	$ 15,442	$ 23,163
10,000 to 24,999	$7,350	$ 14,700	$22,050
5,000 to 9,999	$6,986	$13,972	$20,958
1,000 to 4,999	$6,615	$13,230	$19,845
500 to 999	$4,781	$9,562	$14,343
250 to 499	$3,311	$6,622	$9,933
100 to 249	$2,394	$4,788	$7,182
50 to 99	$1,470	$2,940	$4,410
Up to 49	$924	$1,848	$2,772

The **Trusted Purchasing Alliance (TPA)** serves SLTT governments and nonprofit entities in achieving a greater cybersecurity posture through trusted expert guidance and cost-effective procurement. The TPA builds public and private partnerships and works to enhance collaboration that improves the nation's cyber security posture. The TPA makes cybersecurity purchasing effective, easy and economical.

Pricing is subject to change