Mississippi Department of Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

Craig P. Orgeron, CPM, Ph.D., Executive Director

Notice of Intent to Certify Sole Source

To: Interested Parties

From: Craig P. Orgeron, CPM, Ph.D.

CC: ITS Project Number 49161

Date: August 12, 2025

Re: Sole Source Certification Number 4714 to provide Multi-State Information Sharing and Analysis Center membership for the Mississippi Department of Information Technology Services (ITS)

Contact Name: Vershonda Grindle

Contact Phone Number: 601-432-8213

Contact E-mail Address: Vershonda.grindle@its.ms.gov

Sole Source Certification Award Details

Regarding Information Technology Services (ITS) Sole Source Certification Number 4714 for the Mississippi Department of Information Technology Services (ITS), please be advised that ITS intends to award Center for Internet Security, Inc. (CIS) as the sole source provider of Multi-State Information Sharing and Analysis Center membership for one year in an amount not to exceed $275,000.00. If ITS opts to renew the Multi-State Information Sharing and Analysis Center membership, this sole source certification shall be valid for two additional years. Please be advised that ITS will determine if additional licenses, enhancements, upgrades, and support are within scope during the certification period and may increase the spending authority accordingly. Should Center for Internet Security, Inc. (CIS) change their name during this certification period, then ITS will determine if a recertification is necessary. For an explanation regarding Mississippi state law, policy and procedures for sole source procurements, refer to Attachment B: Sole Source Procurement Overview.

Sole Source Criteria

1. The product or services being purchased must perform a function for which no other product or source of services exist:

   The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the only cyber threat intelligence and incidents response support, real-time alerts, and coordinated defense resources specifically tailored for US State, Local, Tribal, and Territorial (SLTT) governments. The MS-ISAC delivers a unique combination of expertise, trust, scale, access, and mission alignment that cannot be replicated by commercial vendors, or other governmental programs. Members receive carefully vetted and verified threat indicators, including malicious domains and file hashers,

which can be used to automate defenses across their local networks, often without additional equipment. The threat intelligence is directly relevant to the types of systems, vulnerabilities, and threats that specifically target their communities, unlike generic threats that feed from alternative sources. Membership enables timely, direct access to alerts, analysis, and best practices that are not available through any other private or public platform, and creates a unique forum for collaboration and information sharing across all levels of government where best practices are created, shared, and adopted nationwide. This actionable intelligence, designed for state, local, tribal and territorial government context, provides a significant advantage in proactively defending against cyber-attacks.

2. The purchaser must be able to show specific business objectives that can be met only through the unique product or services:

   The services provided by the MS-ISAC are crucial to the State's ability to proactively defend against and respond to cyber threats targeting critical infrastructure and government systems. Benefits from MS-ISAC for the State includes: 24x7x365 Security Operations Center (SOC) offering threat intelligence, detection, and response assistance, regular webinars examining critical and timely cybersecurity issues, access to an annual cybersecurity self-assessment to review cybersecurity maturity, Nationwide Cybersecurity Review (NCSR), cybersecurity tools and resources, including a CIS SecureSuite membership, cybersecurity advisories and notifications, access to secure portals for communication and document sharing, cyber alert maps, weekly top malicious domains/ip reports, and lastly monthly members-only webinars. With ITS purchasing this membership, these benefits will be available to any Mississippi government entity if the entity wishes to participate.

3. The product or services must be available only from the manufacturer and not through resellers who could submit competitive pricing for the product or services:

   The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the only cyber threat intelligence and incident response provider solely tailored to state, local, tribal and territorial governments. No other organization offers the same level of integrated cybersecurity national threat sharing tailored to SLTT governments. The Vendor's sole source certification letter is included as Attachment A.

Schedule

Task	Date
First Advertisement Date	08/12/16
Second Advertisement Date	08/19/16
Response Deadline From Objectors	08/26/16 at 3:00 P.M. Central Time
Notice of Award/No Award Posted	Not before 08/27/16

Project Details

ITS has been utilizing MS-ISAC services since 2005. The MS-ISAC currently includes representatives from all 50 states, more than 18,500 local governments, more than 200 tribal entities and six U.S. territories. To date, ITS has not expended any funds for MS-ISAC services due to it being fully funded by the Federal Department of Homeland Security.

Submission Instructions and Format of Response from Objecting Parties

Interested parties who have reason to believe that the Multi-State Information Sharing and Analysis Center membership should not be certified as a sole source should provide information in the following format for the state to use in determining whether or not to proceed with awarding the Sole Source contract to Center for Internet Security, Inc. (CIS).

1.1 Interested Party Information

1.1.1 Contact Name, Phone Number and email address

1.1.2 Company Website URL, if applicable

1.2 Objection to Sole Source Certification

1.2.1 Interested parties must present specific objections to the Sole Source certification using the criteria listed above.

1.2.2 A statement regarding the Interested Party's capabilities as related to this Sole Source Certification Request.

1.3 Comments will be accepted at any time prior to Tuesday, August 26, 2025, at 3:00 p.m. (Central Time) to Vershonda Grindle at vershonda.grindle@its.ms.gov or at the Mississippi Department of Information Technology Services, 3771 Eastwood Drive, Jackson, Mississippi 39211. Responses may be delivered by hand, via regular mail, overnight delivery, e-mail or by fax. Fax number is (601) 713-6380. ITS WILL NOT BE RESPONSIBLE FOR DELAYS IN THE DELIVERY OF RESPONSES. It is solely the responsibility of the Interested Parties that responses reach ITS on time. Interested Parties may contact Vershonda Grindle to verify the receipt of their Responses. Responses received after the deadline will be rejected.

1.4 Interested Party responses should include the following information:

SUBMITTED IN RESPONSE TO
Sole Source Certification No. 4714-49161
Accepted until August 26, 2025 @ 3:00 p.m.,
ATTENTION: Vershonda Grindle

If you have any questions concerning the information above or if we can be of further assistance, please contact Vershonda Grindle at 601-432-8213 or via email at Vershonda.Grindle@its.ms.gov.

Attachment A: Vendor Correspondence
Attachment B: Sole Source Procurement Overview

Attachment A

31 Tech Valley Drive
East Greenbush, NY 12061 USA
518.266.3460
www.cisecurity.org

To Whom it May Concern:

This letter is in response to your request for a sole source statement for the Multi-State Information Sharing and Analysis Center (MS-ISAC) membership.

Justification for Sole Source Procurement

The MS-ISAC, operated by the Center for Internet Security (CIS), provides cybersecurity threat intelligence, incident response support, real-time alerts, and coordinated defense resources specifically tailored for U.S. State, Local, Tribal, and Territorial (SLTT) governments. The MS-ISAC is recognized as the national Information Sharing and Analysis Center (ISAC) for SLTT cyber readiness and response coordination. This procurement qualifies as a sole source for the following key reasons:

- **Unique Capabilities/Exclusive Provider**: The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the only cyber threat intelligence and incident response provider solely tailored to state, local, tribal and territorial governments. These services are not provided by the federal government. Members receive threat intelligence directly relevant to the types of systems, vulnerabilities, and threats that specifically target their communities, unlike generic threat feeds from alternative sources.

- **Unparalleled Convening Power and Collaboration:** The MS-ISAC currently includes representatives from all 50 states, more than 18,500 local governments, more than 200 tribal entities and six U.S. territories. This vast and diverse membership creates a unique forum for collaboration and information sharing across all levels of government where best practices are created, shared and adopted nationwide. In addition, MS-ISAC can bring together state CIOs, CISOs, city IT directors, tribal government leaders, and federal officials in real-time to respond to emerging threats.

- **No Comparable Alternatives**: No other organization offers the same level of integrated national cybersecurity threat sharing tailored to SLTT governments. The MS-ISAC delivers a unique combination of expertise, trust, scale, access, and mission alignment that cannot be replicated by commercial vendors or other government programs. Members receive carefully vetted and verified threat indicators, including malicious domains and file hashes, which can be used to automate defenses across their local networks, often without additional equipment. This actionable intelligence, designed for state, local, tribal and territorial government context, provides a significant advantage in proactively defending against cyber-attacks.

- **Critical National Infrastructure Role**: Membership enables timely, direct access to alerts, analysis, and best practices that are not available through any other private or public platform.

- **Strategic Partnerships:** MS-ISAC directly collaborates with federal partners and other ISAC organizations to support national security interests.
- **Operational Necessity**: The services provided by the MS-ISAC are crucial to the state's ability to proactively defend against and respond to cyber threats targeting critical infrastructure and government systems.

If you need any further information, please do not hesitate to contact me.

Sincerely,

Carlos Kizzee
carlos.kizzee@cisecurity.org

The acquisition of information technology for all state agencies and institutions of higher learning (IHLs) is within the scope of the ITS law, found in Mississippi Code Section 25-53-1, et seq., and the policies and procedures established in accordance with this statute, found in the ITS Procurement Handbook posted on the ITS website (www.its.ms.gov).

ITS enabling legislation requires that information technology hardware, software and services be acquired in a manner that insures the maximum of competition among all manufacturers and suppliers of such equipment and services. Accordingly, ITS promotes full and open competition through the issuance of open specifications and the objective evaluation of Interested Party proposals to determine the lowest and best offering to meet an agency's or public university's business requirements. True competition protects the integrity and credibility of purchasing in the public sector and is essential in providing best value and adequate contractual protection for the purchasing entity. In certain limited situations, information technology acquisitions may be sole-sourced.

ITS utilizes the provisions of Public Purchasing Law for Sole Source and Emergency procurements of information technology. Mississippi Public Purchasing Law (Mississippi Code Section 31-7-13) specifies that noncompetitive items available from one source only be exempted from bid requirements (sole-sourced). ITS statute, in Section 25-53-5 (p), permits ITS to utilize provisions in Public Purchasing Law or regulations, when applicable.

Per Public Purchasing law, acquisitions must meet the following criteria to be authorized as sole source:

1. The product or services being purchased must perform a function for which no other product or source of services exists,

2. The purchaser must be able to show specific business objectives that can be met only through the unique product or services, AND

3. The product or services must be available only from the manufacturer and NOT through resellers who could submit competitive pricing for the product or services. The vendor's correspondence regarding this criterion for this project is included as Attachment A.

By policy as documented in the ITS Procurement Handbook, acquisitions of IT services must include the following information to be authorized as sole source:

1. An explanation about why the amount to be expended is reasonable, and

2. An explanation regarding the efforts by the purchaser to obtain the best possible price.

For state agencies, approval of all technology purchases with a lifecycle cost of $5,000 or less, including sole source purchases, has been delegated to the agency. The ITS Procurement Limits Policies for Agencies (a section in the ITS Procurement Handbook) require a minimum of two competitive written bids or proposals for technology purchases with a lifecycle cost over $5,000 but not over $75,000 (not over $25,000 for projects funded by the American Recovery and Reinvestment Act). Since, for single source items, the procuring agency will be unable to obtain two written bids, ITS must certify all sole source acquisitions of information technology with a lifecycle cost greater than $5,000.

Institutions of Higher Learning (IHLs) or public universities have been delegated the authority to certify sole source procurements up to $250,000 lifecycle cost under the ITS Procurement Limits Policies for IHLs (a section in the ITS Procurement Handbook). For the certification of sole source procurements delegated to the CIOs at public universities, the public university must follow ITS' Sole Source Procedure, including advertisement of the intent to award as sole source. Institutions certifying a sole source purchase must ensure the criteria listed above are met and documented in writing by the institution and the Interested Party prior to certifying a product or service as sole source. Sole source documentation must be reviewed and approved by the IHL's CIO for any sole-source certification above $5,000. All sole source documentation should be retained in the public university's procurement file. Sole source requests above $250,000 lifecycle cost require ITS approval.

Other than the delegations outlined above, all sole source technology procurements must be certified by ITS.

ITS thoroughly reviews Sole Source Certification Requests, determining if competing products and/or services exist. If so, ITS conducts a competitive procurement. If ITS' review confirms the sole source, then a Sole Source advertisement is issued, giving other Interested Parties an opportunity to identify competing products and/or services. Based upon the results of the Sole Source advertisement, ITS will either certify the request as a sole source or conduct a competitive procurement.