



Texas Department of Information Resources
Transforming How Texas Government Serves Texans

TX-ISA0 Portal User Guide

Version 3.0

September 8, 2023

Overview

The Texas Information Sharing and Analysis Organization (TX-ISAO) provides a forum for entities in Texas, including state agencies, local governments, public and private institutions of higher education, and the private sector, to share information regarding cybersecurity threats, best practices, and remediation strategies. TX-ISAO members have access to the TX-ISAO threat portal which provides an efficient and secure method to share indicators of compromise (IOCs) and other actionable intelligence, and contains current threat bulletins, a library of archived bulletins, and upcoming events. Members are also able to share best practices, lessons learned, and insights through the discussion module.

Table of Contents

Overview	2
Logging In.....	4
First-Time Users.....	4
After TDIS Enrollment	4
Announcements Module.....	8
Receiving Announcements.....	8
Announcement Fields	8
Viewing Announcements.....	9
Announcements by Type.....	12
Events	14
Discussion Module.....	16
Creating a New Discussion.....	16
Viewing or Replying to Discussions.....	17
Viewing Recently Published Discussions	18
Search Function.....	20
Other TX-ISAO Portal Activities	21
Submit a Threat Report	21
Manage Email Subscriptions	21
TX-ISAO Portal Support Requests	22

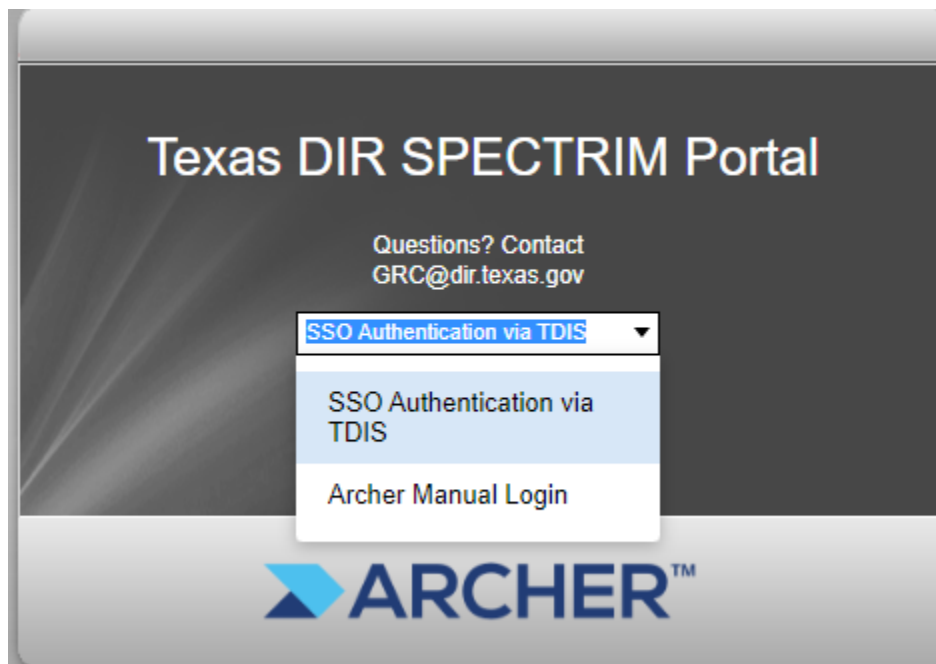
Logging In

First-Time Users

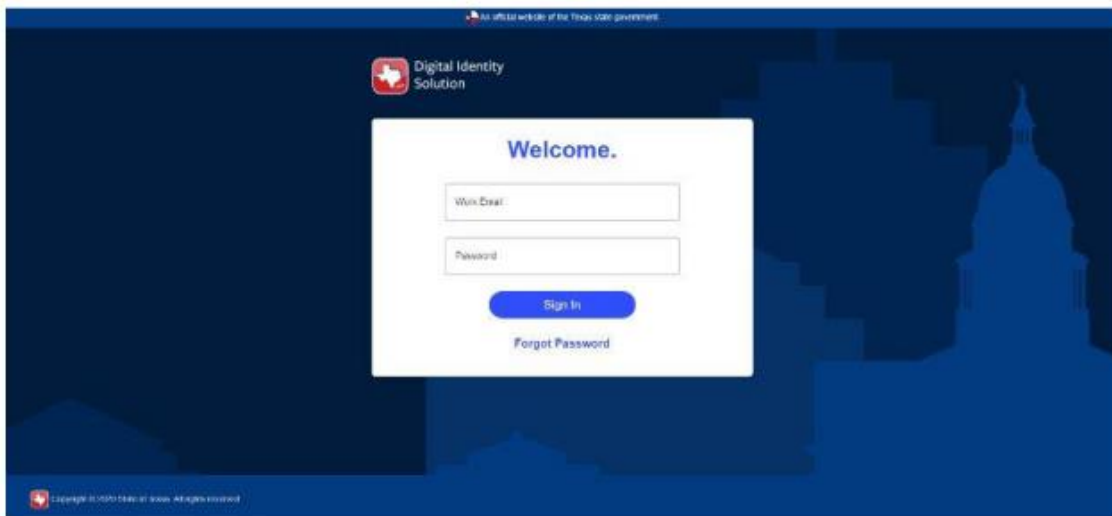
1. If this is your first-time logging into the TX-ISAO Portal, you will start by performing the enrollment process in the Texas.gov Digital Identity Solution (TDIS). Refer to the Enrollment Quick Reference Guide for details: <https://dir.texas.gov/resource-library-item/tdis-enrollment-quick-reference-guide>.
2. After completing TDIS enrollment, proceed with step 6 in the section "Logging In (after TDIS enrollment)".

After TDIS Enrollment

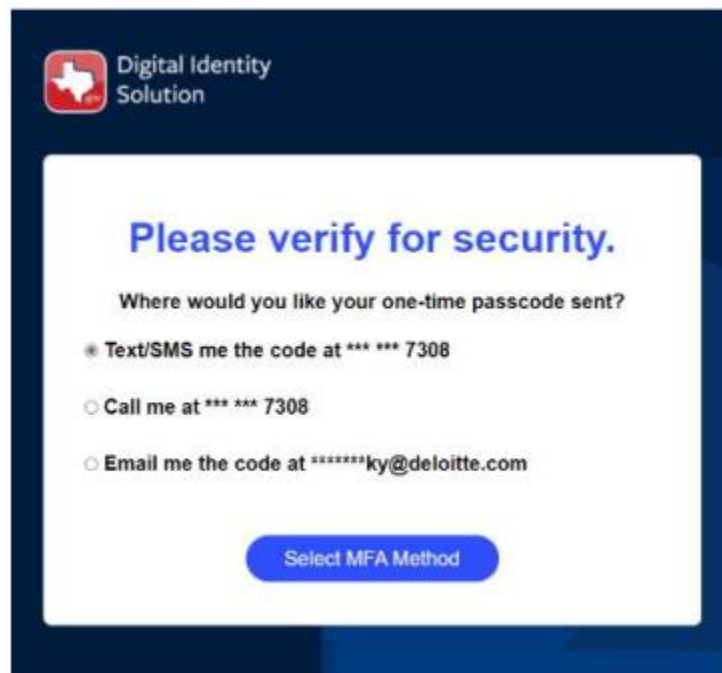
1. Navigate to the TX-ISAO Portal <https://dir.archerirm.us>.
2. You will see the login options below. Choose **SSO (Single Sign-On) Authentication via TDIS** and click **Login**.



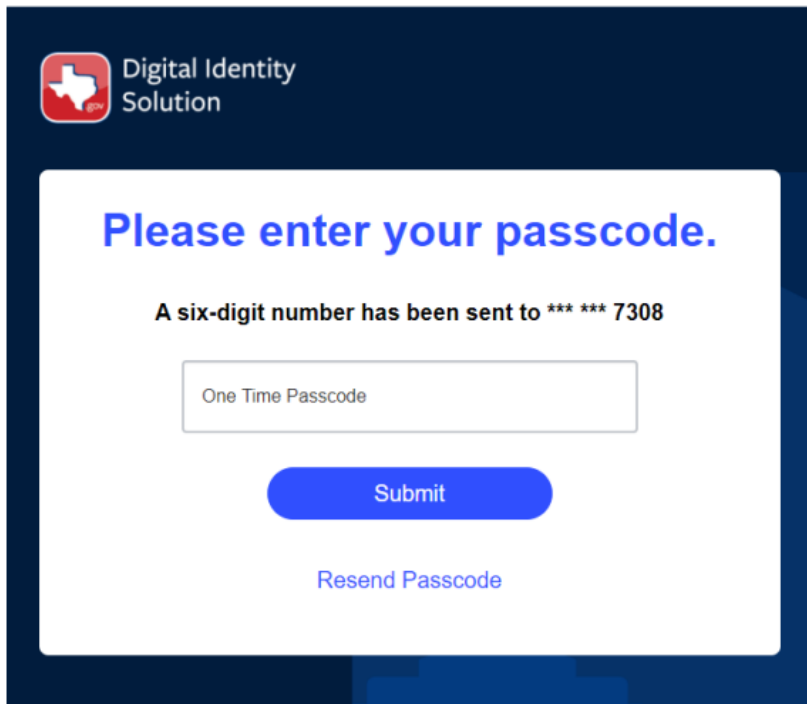
3. You will be redirected to the TDIS login page. Begin login via TDIS by entering your email and password.



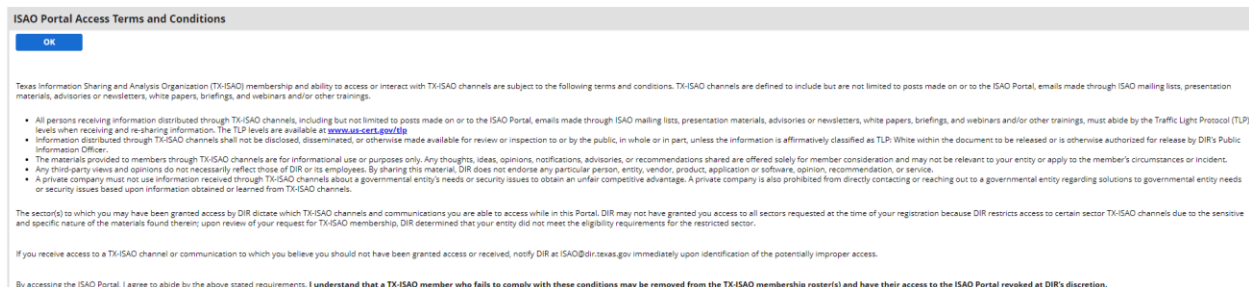
4. You will then be prompted to verify your identity by providing a numeric, One-Time Passcode (OTP) via your preferred MFA method. Options will vary depending on which MFA methods you have registered. Once you have made your MFA selection, click **Select MFA Method**.



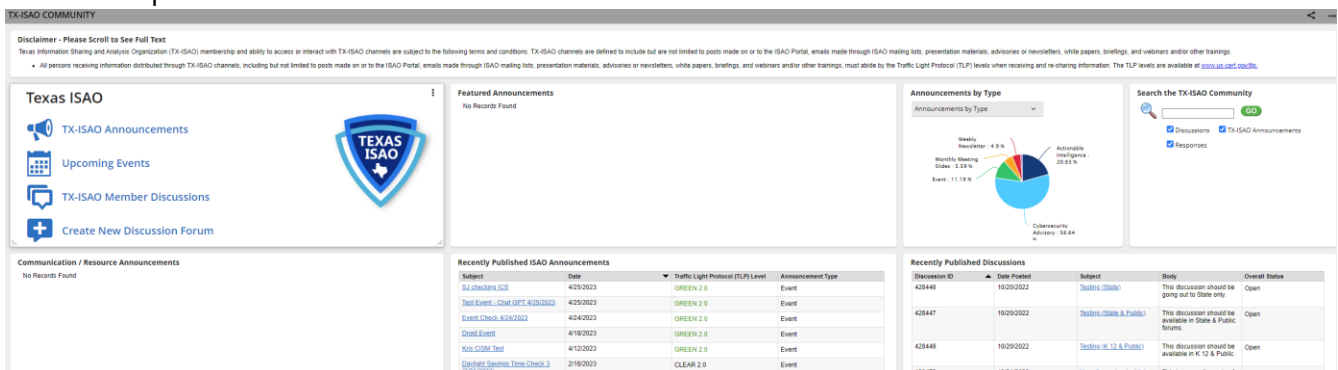
5. Enter the passcode into the OTP field. Click **Submit** to proceed. Please note, this passcode expires in five minutes. If you cannot locate the passcode, if it does not arrive, or expires before it is entered, you may request a new OTP to be sent by clicking Resend Passcode.



- You will then be directed back to the TX-ISAO Portal. If this is your first time logging in, you will need to review and accept the ISAO Portal Access Terms and Conditions by selecting **OK** after reading. (Note: The disclaimer will also be displayed at the top of the home page. On the home page, use the scroll bars to view the full disclaimer. You can also collapse the disclaimer by clicking the ellipsis in the upper right corner.)



- Once logged in, your dashboard will look like this. From here you can access the modules of the portal.



- a. The TX-ISAO Portal is built onto the SPECTRIM platform, so if you are a TX-ISAO member who uses SPECTRIM for GRC activities, you may need to select the **TX-ISAO** module from the ellipsis on the upper right of your dashboard.



Announcements Module

Receiving Announcements

1. Announcements are distributed through the TX-ISAO Portal via email, from (Texas ISAO - Do Not Reply noreply@archerirm.us). Most announcements are distributed with the full detail (i.e., Full Announcement), and any supporting documents included in the email. In these emails, the subject line is a link to the announcement in the TX-ISAO Portal.

ANNOUNCEMENT INFORMATION

TLP: CLEAR
Distribution Limits

TLP: CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure.

Announcement ID: 1231000

Announcement Standard Importance: Date: 4/25/2023

Announcement Type: Cybersecurity Advisory

Topic Tags:

Subject: Abuse of the Service Location Protocol May Lead to DoS Attacks

Description: The Service Location Protocol (SLP, [RFC 2608](#)) allows an unauthenticated remote attacker to register arbitrary services. This could allow an attacker to use [spoofed UDP traffic](#) to conduct a denial-of-service (DoS) attack with a significant amplification factor.

Researchers from [Bitsight and Curesec](#) have discovered a way to abuse SLP—identified as CVE-2023-29552—to conduct high amplification factor DoS attacks using spoofed source addresses.

2. Some more sensitive announcements will be distributed as a notification that an announcement has been published. These notifications will include the subject line only and you will need to log into the TX-ISAO Portal to access the announcement details and any supporting documents. Click the subject line or the link in the email to be directed to the TX-ISAO Portal. After logging in, you will be able to access the announcement.

SUBJECT: [Texas ISAO Monthly Meeting Slides](#)

TLP: GREEN

Announcement ID: 428115

Date: 9/29/2022

Announcement Type: Monthly Meeting Slides

Importance: Standard

Distributed to: TX-ISAO: K-12 Education

For full information, please access the announcement at the following link:

<https://dir-dev.archer.rsa.com/default.aspx?requestUrl=.%2fGenericContent%2fRecord.aspx%3fid%3d428115%26moduleId%3d591>

Announcement Fields

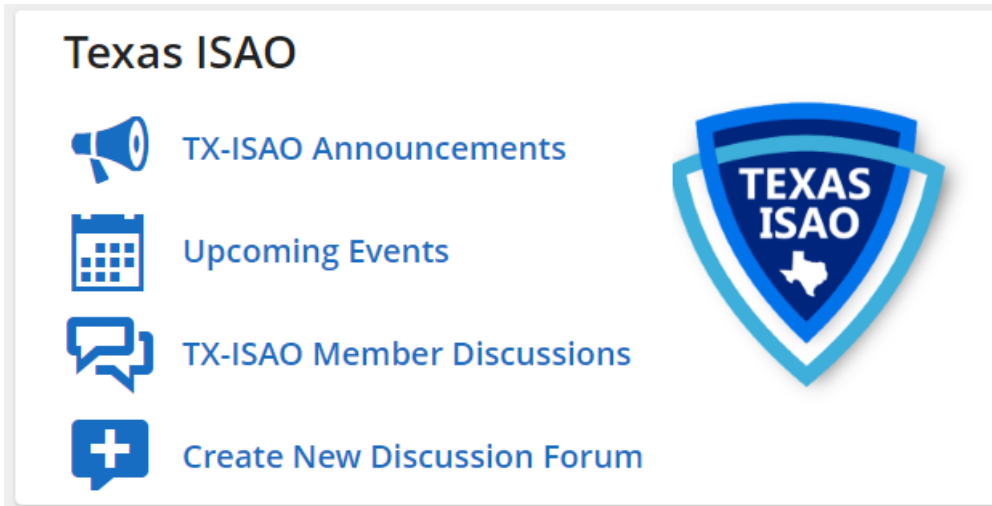
Announcements encompass a variety of communications (ex. security advisories, events, and meeting slide decks) and are distributed through the TX-ISAO Portal. Announcements contain the following fields. (Events include a few additional fields. Refer to the Events section for details.)

1. TLP (Traffic Light Protocol) – specifies guidelines for sharing
 - a. Red: Not for disclosure, restricted to participants only
 - b. Amber+Strict: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization

- c. Amber: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients
 - d. Green: Limited disclosure, recipients can spread this within their community.
 - e. Clear: Recipients can spread this to the world, there is no limit on disclosure.
2. Announcement ID – unique ID assigned to each announcement
3. Announcement Type – categorizes the type of information in the announcement
 - a. Actionable Intelligence: Specific intelligence that can be acted upon to mitigate risk of attacks (Ex. CyOps Weekly Intel Report, Malicious IPs)
 - b. Cybersecurity Advisory: General intelligence with information about a known vulnerability (Ex. MS-ISAC Advisories, CISA Advisories, Vulnerabilities)
 - c. Event: Webinars and in-person events (Ex: TX-ISAO Monthly Meeting, OCISO Educational Webinars, Annual Information Security Forum (ISF), Training Opportunities)
 - d. Monthly Meeting Slides: Slide decks from webinars or in-person events
 - e. Weekly Newsletter: Texas ISAO Weekly
 - f. Resources: Documents available for use by TX-ISAO members (Ex: Tabletop exercise materials)
 - g. Communications: General messages from OCISO
 - h. Other: Announcements that do not fit into another defined category
4. Date – the date the announcement was published
5. Importance – provides guidelines for prioritizing the information in the announcement
 - a. Standard: General intelligence or events. Follow your standard process for analyzing and taking any necessary actions.
 - b. Critical: Intelligence or events that may require an expedited response. Consider prioritizing these items as they may pose a higher risk to your organization.
6. Topic Tags (if applicable) – groups announcements that address a similar topic
7. Subject – announcement title
8. Description – detailed information for the announcement (Note: sometimes this will be included in the email distribution, and sometimes you will need to log into the portal to view it)
9. Supporting Attachments (if applicable) – documents associated with the announcement (Note: sometimes this will be included in the email distribution, and sometimes you will need to log into the portal to view it)

Viewing Announcements

1. From the home screen, select **TX-ISAO Announcements**.



2. You will be taken to a listing of announcements.



3. On the left side of the screen, refine your search by selecting one or more checkboxes in the Traffic Light Protocol (TLP), Date, Announcement Status, Announcement Type and/or Topic Tags. Click the **Apply** button at the bottom left to see the updated list.
 - a. Announcements that were distributed before September 2022, were imported into the TX-ISAO Portal and have an announcement status of Archived. Please note that these announcements were imported as text and may not include formatting.

▼ **Traffic Light Protocol (T...**

- WHITE 1.0 (143)
- GREEN 1.0 (101)
- AMBER 1.0 (56)
- GREEN 2.0 (14)
- RED 1.0 (11)
- CLEAR 2.0 (11)
- AMBER+STRICT 2.0 (2)
- AMBER 2.0 (2)

▶ **Date**

▶ **Announcement Status**

▼ **Announcement Type**

- Cybersecurity Advisory (172)
- Actionable Intelligence (62)
- Event (48)
- Weekly Newsletter (23)
- Monthly Meeting Slides (18)
- Other (15)
- Communications (1)
- Resources (1)

▶ **Topic Tags**

4. Click the subject line of an announcement to see the details. Any attachments will be shown at the bottom of the screen in the section **Supporting Attachments**.

ANNOUNCEMENT INFORMATION

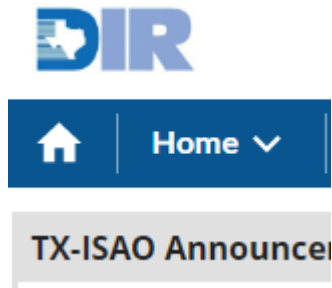
TLP: CLEAR

Distribution Limits

TLP: CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure.

<p>Announcement ID: 474438</p> <p>Announcement Standard Importance:</p> <p>Announcement Type: Actionable Intelligence</p> <p>Topic Tags:</p> <p>Subject: Multiple Vulnerabilities in VMware vRealize Log Insight Could Allow for Remote Code Execution</p> <p>Description:</p> <p>SUBJECT: Multiple vulnerabilities in VMware vRealize Log Insight Could Allow for Remote Code Execution</p>	<p>Date: 1/31/2023</p>
--	------------------------

- Select the **House** icon in the upper left to return to the home screen.



- From the dashboard, you can access individual announcements through the Featured Announcements or Recently Published ISAO Announcements workspaces. You can also use the Announcements by Type pie chart at the bottom left (see next section for details).

Featured Announcements

Subject	Featured Announcement Start Date	Featured Announcement End Date	Announcement Type
CyberOps Intel Week of April 17, 2023 through April 24, 2023	4/24/2023	4/30/2023	Actionable Intelligence
OCISO Educational Webinar: Lufkin ISD presents Data Security and Management Best Practice Considerations	4/5/2023	5/3/2023	Event
DIR & Gartner Security webinar: Privacy and the Importance of Compliance	4/4/2023	4/27/2023	Event

Page 1 of 1 (3 records)

Recently Published ISAO Announcements

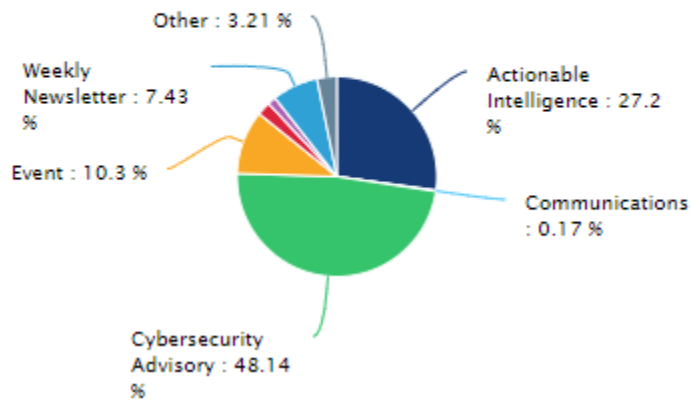
Multiple Vulnerabilities in PaperCut NG/MF Could Allow for Remote Code Execution	4/22/2023	CLEAR 2.0	Cybersecurity Advisory
VMware Releases Security Update for Aria Operations for Logs	4/21/2023	CLEAR 2.0	Cybersecurity Advisory
Oracle Releases Security Updates	4/21/2023	CLEAR 2.0	Cybersecurity Advisory
Drupal Releases Security Advisory to Address Vulnerability in Drupal Core	4/21/2023	CLEAR 2.0	Cybersecurity Advisory
Active Exploitation of Vulnerabilities Found in PaperCut MF/NG Servers	4/21/2023	CLEAR 2.0	Cybersecurity Advisory
Cisco Releases Security Advisories for Multiple Products	4/21/2023	CLEAR 2.0	Cybersecurity Advisory

Announcements by Type

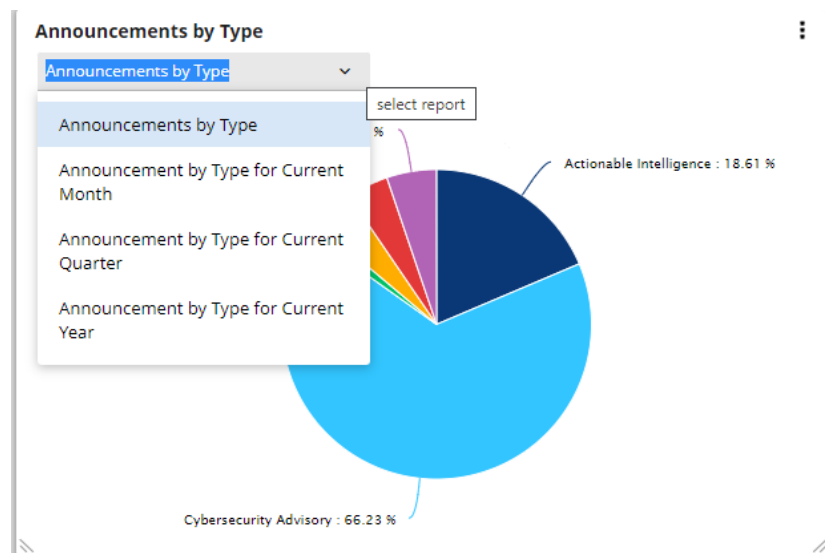
- The Announcements by Type pie chart shows the overall percentage of each announcement type. To view the details, select the area in the pie chart you want to view. You will be taken to the listing of announcements for that announcement type. Click the subject line of any announcement to see the details.

Announcements by Type

Announcements by Type ▼

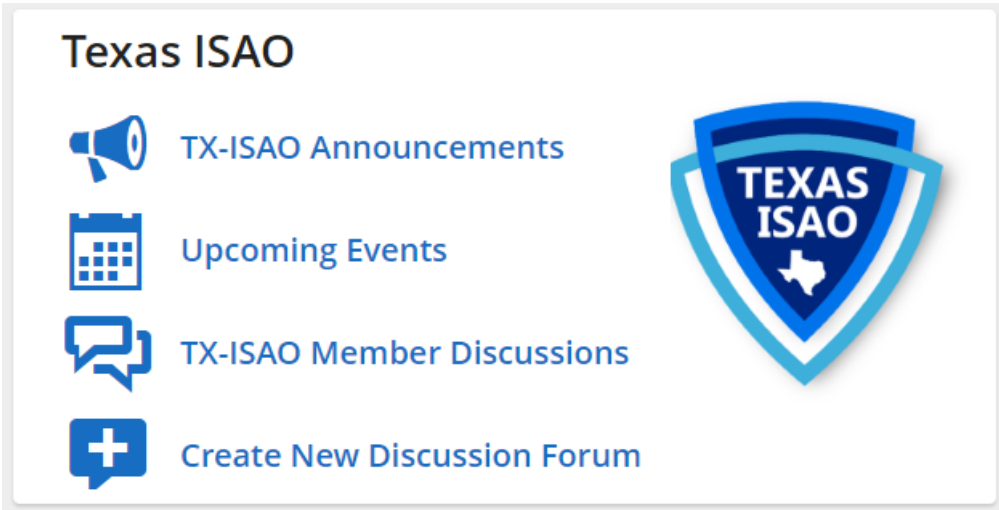


- The default pie charts show **Announcements by Type** for all published and archived announcements. You can also filter the pie chart by changing the drop-down to show Announcements by Type for the Current Month, Current Quarter, or Current Year.

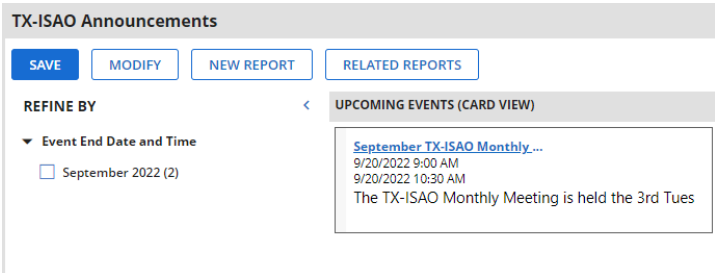


Events

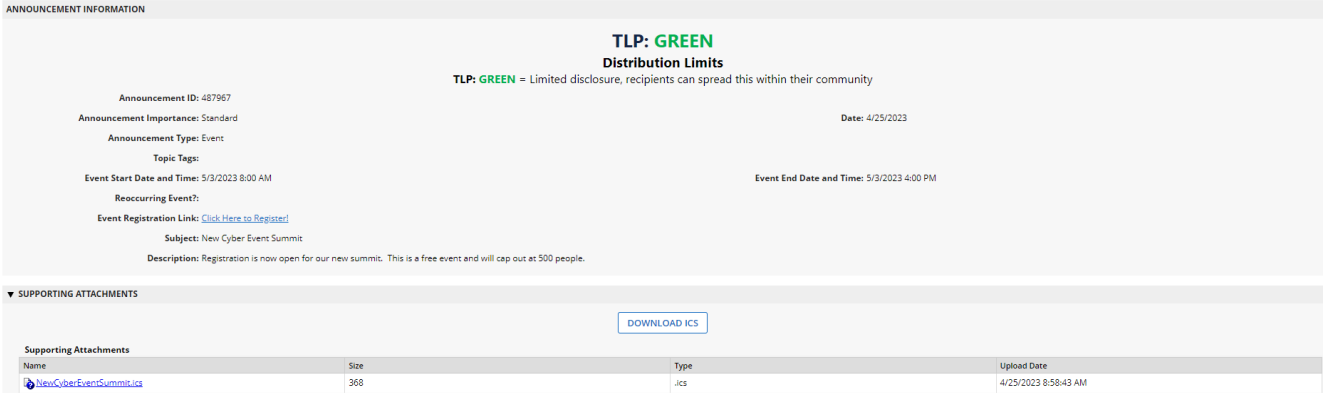
1. From the home screen, select **Upcoming Events**.



2. You will be taken to the calendar screen below in card view.



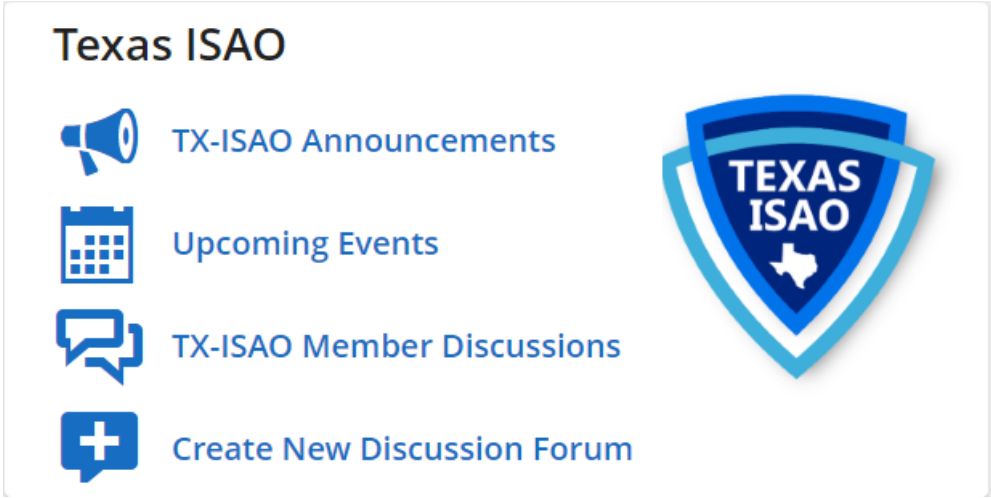
3. Click the event title to view the event details. In addition to the standard announcement fields, you will also see:
- a. Event Start Date and Time
 - b. Event Registration Link or Join Link (if applicable)
 - c. Event End Date and Time
 - d. Download ICS button – Click to download an ICS file to your calendar. The ICS file may also be included as a Supporting Attachment.



4. You can also refine the list of upcoming events by month.

Creating a New Discussion

- 1. To create a new discussion, choose **Create New Discussion Forum** from the **Texas ISAO** Menu.



- 2. When choosing this option, you will see the **DISCUSSION FORUM TERMS AND CONDITIONS** and **STAGE INFORMATION**. In the **DISCUSSION TOPIC** section, you will enter the **Subject** heading and then the **Body** of your post. Then you will select the sector(s) you wish to post to in the **DISCUSSION OWNER ACTIONS** and add any **SUPPORTING DOCUMENTATION**. You can also reference a **Related Announcement** by using the **Lookup function**. Then select the record you would like to reference on the next screen.

DISCUSSION TOPIC

Discussion ID: _____ Date Posted: _____
+ Subject: Overall Status: Open
+ Body:

Posted By: _____ Topic Tags: ...
Number of Replies in Thread: _____

Related Announcement Lookup

Subject
No Records Found

Record Lookup

Search Results Show Filters

Search:

Drag a column name here to group the items by the values within that column.

<input type="checkbox"/> Subject
<input type="checkbox"/> #StopRansomware: MedusaLocker & Multiple Vulnerabilities in Mozilla Products Could Allow for Arbitrary Code Execution
<input type="checkbox"/> (MN) Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution & Proxies and Configurations Used for Credential Stuffing Attacks on Online Customer Accounts
<input type="checkbox"/> [TX-ISAO-State] InfoSec Academy Course Announcement Developer Offerings: EC Council Certified Application Engineer (CASE) Java Training 7/18-20
<input type="checkbox"/> A Backdoor in WordPress AccessPress Plugins and Themes Could Allow an Attacker Access to a Targeted Website

- When you are ready to post your discussion, you can choose either **SAVE** or **SAVE AND CLOSE** in order to complete your new record. If you get a reply to your discussion, you will receive an email notification and can access it through the portal. When you no longer wish to receive replies, you can close the discussion by changing the **Discussion Status**. If applicable, you can also report a **Discussion Conclusion**.

Discussions: Add New Record

▼ DISCUSSION OWNER ACTIONS

Discussion Status: Open Closed

Limited Discussion TX-ISAO: Public Sector TX-ISAO: State Government

Access To:

▼ DISCUSSION OWNER ACTIONS

Discussion Status: Open Closed

Limited Discussion TX-ISAO: Public Sector TX-ISAO: State Government

Access To:





Discussion Conclusion:


Closed Date:

Viewing or Replying to Discussions

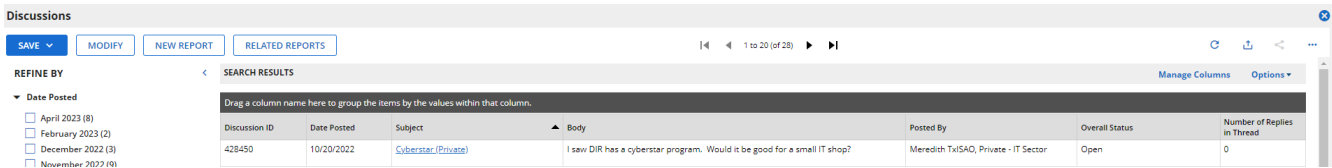
- You will receive an email when a discussion has been posted to your sector(s). To access the discussion module, click the link in the email or choose **TX-ISAO Member Discussions** from the **Texas ISAO** menu.

Texas ISAO

-  TX-ISAO Announcements
-  Upcoming Events
-  TX-ISAO Member Discussions
-  Create New Discussion Forum



- By choosing **TX-ISAO Member Discussions**, you will be taken to a list of discussions that have been published to your sector.



- You can then choose a discussion to view the details or reply by clicking the subject link. The **DISCUSSION FORUM TERMS AND CONDITIONS** and **STAGE INFORMATION** will show at the top of your screen with the **DISCUSSION TOPIC** and ability to **REPLY** below. By clicking **ADD NEW** in the **REPLY** section, you can create a reply that the discussion owner will be able to see.
- You can also click **REPORT DISCUSSION POSTING TO ISAO MODERATOR** if you feel that the discussion does not align with the stated terms and conditions.

DISCUSSION FORUM TERMS AND CONDITIONS

Your participation in the ISAO Discussion Forum (Discussion Forums) constitutes your acknowledgment of and agreement to the following terms and conditions:

- DIR neither reviews or screens any posts or messages nor verifies the content of any post or message made by ISAO members in the Discussion Forums prior to posting.
- DIR reserves the right to delete any post or message it considers inappropriate.
- DIR reserves the right to deny or revoke access to the Discussion Forums to anyone who violates the Discussion Forums or ISAO Portal terms and conditions.
- Any opinions expressed by Discussion Forum participants are their own. They do not necessarily reflect those of DIR.
- All posts, messages, and information posted, accessed, or transmitted in the Discussion Forums are offered "as is" without any endorsements, guarantees, or warranties by DIR.
- You shall not post or transmit any unlawful, threatening, abusive, libelous, defamatory, obscene, pornographic, profane, or otherwise objectionable information of any kind, including, but not limited to, any posts, messages, or other transmissions constituting or encouraging conduct that may be considered a criminal offense, give rise to civil liability, or otherwise violate any local, state, national, or international law. Any ISAO member who does so may have their right of access to the Discussion Forums or the ISAO Portal automatically revoked without notification.
- You shall not post, message, or transmit any information or software that contains a virus or other harmful component. This prohibition extends to posts or messages that include links to sites, software, or applications that contain a virus or other harmful component.
- You shall not make or send any posts, message, or information that violates the copyright, trademark, trade secret, privacy, or publicity rights of any third party.
- By participating in a Discussion Forum, you are agreeing that all posts or messages read, reviewed, or accessed will be used only for informational, educational, or professional purposes. Any information that you disclose in a Discussion Forum may be read, viewed, or obtained by any other ISAO member(s) approved to access the forum sector(s).
- There may be no commercial or other unauthorized use of the Discussion Forum participant lists. You shall not use the Discussion Forums to exchange information, services, materials, or software in return for payment of any kind (trade of like items, special discounts, cash, etc.) nor shall you use the Discussion Forums to solicit, promote, or otherwise market any services, software, or application in which you have an interest. You shall not use any information received through the Discussion Forums to cultivate outreach or marketing campaigns for prospective customers. This includes, but is not limited to, the creation of a mailing or contact list targeting ISAO members who have identified specific issues on the ISAO Portal or Discussion Forums.
- By posting a message to a Discussion Forum, you grant DIR a non-exclusive license to copy and distribute the posting. An ISAO member is prohibited from distributing or transmitting, orally or in writing, messages or information posted by other ISAO members without the express written permission of DIR and the member.

STAGE INFORMATION

During this stage, Discussion Owner/Discussion Participants will respond to the discussion and Discussion Owner will update the discussion status appropriately. [Open](#)

To respond to a discussion, click on **Add New** at the top right corner of the **Reply** cross-reference section.

Discussion Owner can change the status of the discussion. To change the status of the discussion, complete the following steps:

- To Close a discussion:
 - Change **Discussion Status** to **Closed** in Discussion Owner Actions section.
 - Provide **Discussion Conclusion**, if any.
 - Click Save in the Record Toolbar.
- Overall Status** for the discussion and related responses will change to **Closed**. Closed Date will be set to current day.

[REPORT DISCUSSION POSTING TO ISAO MODERATOR](#)

DISCUSSION TOPIC

Discussion ID: 428470 Date Posted: 10/21/2022

Subject: New discussion (public) Overall Status: Open

Body: This is a new discussion for the public sector, referencing an announcement that is state only.

Posted By: Meredith TxISAO, State Agency Topic Tags:

Number of Replies in Thread: 1

Related Announcement

Subject: [State only cybersecurity advisory](#)

REPLY [Add New](#)

Subject	Body	Created By
Reply to New Discussion	I have received this with my state account.	ISAOSate, Kris

Viewing Recently Published Discussions

- There is a section of the dashboard – **Recently Published Discussions**. Here you can see all discussion that have been published to your sector(s).
- Click the Subject line to view the discussion details.

Recently Published Discussions



Discussion ID	Date Posted	Subject	Body	Overall Status
428446	10/20/2022	Testing (State)	This discussion should be going out to State only.	Open
428447	10/20/2022	Testing (State & Public)	This discussion should be available in State & Public forums.	Open

Search Function

1. From the dashboard, you can search discussions, announcements or responses for specific terms. You can also search for a specific announcement if you know the announcement ID. Locate the Search the TX-ISAO Community workspace. Enter your search term(s) and click **GO**.



The screenshot shows a search interface titled "Search the TX-ISAO Community". It features a magnifying glass icon on the left of a search input field. To the right of the input field is a green "GO" button. Below the input field, there are three checked checkboxes: "Discussions", "TX-ISAO Announcements", and "Responses".

2. Your search will then bring up results that match the search term(s). Click the subject line to see the details.

Other TX-ISAO Portal Activities

Submit a Threat Report

1. If you want to report a cyber threat for possible research and dissemination, click the **Submit a Threat Report** in the Quick Links section, or navigate to the following site:
<https://dircommunity.force.com/isaothreatreport/s/report>.

[Quick Links](#) [View Announcements](#) [Submit a Threat Report](#) [Manage Email Subscriptions](#) [Contact Texas ISAO](#)

Manage Email Subscriptions

1. You can manage your email subscriptions by clicking the **Manage Email Subscriptions** link.

[Quick Links](#) [View Announcements](#) [Submit a Threat Report](#) [Manage Email Subscriptions](#) [Contact Texas ISAO](#)

2. You will see the following basic email subscriptions. You have the ability to subscribe to and unsubscribe from announcements using a wide range of options including TLP level and distribution type. If you unsubscribe from a specific announcement type, you will not receive an email notification when those announcements are published. If the **Subscribed** checkbox is grayed out, you are unable to unsubscribe from that announce type.

Manage Email Subscriptions

SAVE

Email Subscriptions ⓘ

Subscribed ▾	Name ▾	Application ▾	Frequency ▾
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: GREEN: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: GREEN: Subject Line Only	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: WHITE: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: WHITE: Subject Line Only	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: RED: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Weekly Newsletter Preview: Admin Notification	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	Immediate TX-ISAO Announcements: TLP: GREEN: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	Immediate TX-ISAO Announcements: TLP: RED: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	Immediate TX-ISAO Announcements: TLP: WHITE: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: AMBER: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	Immediate TX-ISAO Announcements: TLP: AMBER: Full Announcement Text	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: AMBER: Subject Line Only	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Announcements: TLP: RED: Subject Line Only	TX-ISAO Announcements	Instantly
<input type="checkbox"/>	Daily Digest TX-ISAO Announcements	TX-ISAO Announcements	Instantly
<input checked="" type="checkbox"/>	TX-ISAO Weekly Newsletter	TX-ISAO Announcements	Instantly

3. All boxes are checked by default, except for Daily Digest TX-ISAO Announcements. This option, when checked, will send a daily email that includes all the preceding day's announcement notifications. The digest will include all announcement types that you are eligible to receive except those that you have unsubscribed from.
4. When making any changes, make sure to click **SAVE** in the upper left corner under the Manage Email Subscriptions header.

TX-ISAO Portal Support Requests

For TX-ISAO Portal technical assistance, click the **Contact Texas ISAO** link or email DIRSecurity@dir.texas.gov.

[Quick Links](#) [View Announcements](#) [Submit a Threat Report](#) [Manage Email Subscriptions](#) [Contact Texas ISAO](#)