TEXAS CYBER COMMAND

Texas Information Sharing and Analysis Organization (TX-ISAO)

Member User Guide for CSAP

TEXAS CYBER COMMAND

Version 4.0

November 2026

Table of Contents

Overview **2**

Enrollment **2**

Register Your Account 2

Mobile App Setup 3

TX-ISAO Alerts **4**

Accessing Alerts 4

Alert Notifications (Email & SMS) 5

Share Threat Intel **6**

Request for Information **8**

Events **9**

Accessing Events 9

TXCC Monthly Meetings 10

View Past Event Submissions 12

GRC Hub **12**

Accessing the GRC Hub 12

GRC Hub Submissions 14

Traffic Light Protocol **16**

Need Help **16**

Overview

The Texas Cyber Command (TXCC) has migrated the Texas Information Sharing and Analysis Organization (TX-ISAO) Portal to the Cyware Situation Awareness Platform (CSAP). The TX-ISAO Portal 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 Portal. This portal 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.

Enrollment

To enroll in the TX-ISAO, complete and submit the TX-ISAO Form.

Register Your Account

Once a Texas Cyber Command (TXCC) analyst enrolls you in the platform:

1. You will receive an invite email from Cyware <no-reply@cyware.com> to the email you provided. This e-mail will include your registration link. **The registration link will expire within 72 hours (three calendar days).**
2. If you attempt to register your account after the link expires, you can use Cyware's **Forgot Password** function to complete your registration. This option will only work if an account has been created for you by TXCC. Follow these steps to use the Forgot Password function:
    i. Navigate to **TX-ISAO Portal**.
    ii. Select Forgot Password
    iii. Enter your email address, and an email containing your password reset link will be sent. If you didn't receive the email, check your Spam folder or try again. If you are still unable to login, contact TX-ISAO@txcc.texas.gov for assistance.
3. Select the **registration link provided in the invitation**. A browser screen will open for you to move onto the next step.
4. Create your password, then **log into the portal**.
5. Select your **Country** and **State**, then select **Continue**.
6. Select either **IT Professional** or **General User**, then select **Next**.
7. Enter your name (if not already populated), job title, phone number, address, and select **Next**.
8. Enable push notifications for the alert categories you want to receive, then select **Next**.
9. **Admin Enabled Categories** cannot be fully disabled, but you can turn off their e-mail and mobile notifications. **Note:** This alert will still appear on your member dashboard.

Important: In the **Optional Category** section, if you disable the **Alert** option, you will **NOT** receive notifications for this category nor will you be able to view that category's alert in your member dashboard.

10. Enter your Crisis Profile Information, then select **Next**.
    a. The **Crisis Profile** is a feature that allows you to configure your Crisis Notification call and SMS preferences according to your working hours. This ensures that during a cybersecurity emergency, crisis alerts reach members through the right contact channels at the right time.

Note: Without a configured Crisis Profile, you will only receive **crisis notification alerts** via email. Voice calls and SMS will not be delivered to you.

    b. If you add **multiple contact numbers**, you must set call priority order for each of these three scenarios:
        i. Weekdays (during business hours)
        ii. Weekdays (after business hours)
        iii. Weekends
    c. When a crisis alert is triggered:
        i. The system calls/texts the First Priority contact.
        ii. If there is no response, it escalates to the Second Priority contact.
        iii. If there is no response, it escalates to the Third Priority contact.
11. Choose your preferred layout, then select **Finish**.
12. You will be shown a short tutorial of the dashboard. This step concludes your enrollment.

Mobile App Setup

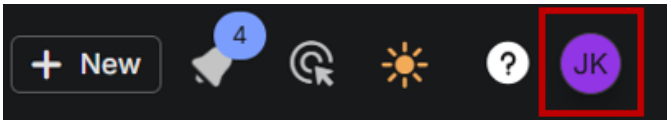
The TX-ISAO Portal now allows mobile notifications through the CSAP mobile application.

Disclaimer: *Access to and use of this mobile application may be subject to your organization's network, security, or information technology policies and controls. Some organizations may restrict or block access to this application. If you are unable to access or use this application, contact your organization's IT department or appropriate system administrator for assistance.*

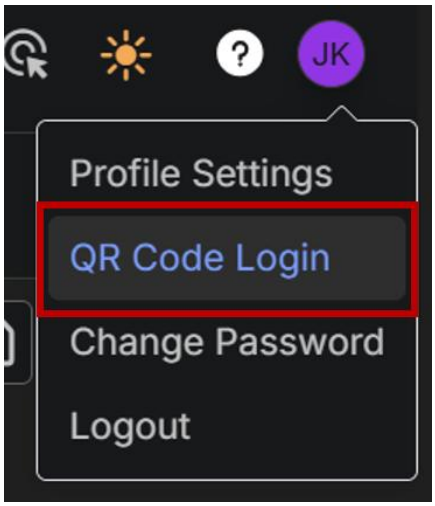
To setup the mobile app:

1. Download the **Cyware Enterprise app** from your phone's designated app store.
2. Use one of the following two methods to login:
    a. **Access Code Login**
        i. Open the **Cyware Enterprise app** on your phone.
        ii. Enter your **organization access code** (included in your email invite) and select **Continue**.
        iii. Enter your **username and password**, then select **Continue**.
        iv. Enter the **One-Time Passcode** sent to your email or authenticator app, then select **Sign In To CSAP**.
    b. **QR Code Login:**
        i. Sign in to the TX-ISAO Portal from your computer.

ii. Go to **User Profile** by selecting your initials in the top-right corner of the screen.



iii. Select **QR Code Login**. A dynamic QR code will then be displayed.



iv. Open the **Cyware Enterprise app**.
v. Select **QR CODE** on the login screen.
vi. **Scan** the QR code with your mobile camera.
vii. You will automatically be signed in.

13. Make sure you **enable the push notifications** you want to receive to your mobile app.
    c. See the Alert Notifications section for the steps to enable or disable push notifications.

TX-ISAO Alerts

Accessing Alerts

1. Sign in to the TX-ISAO Portal.
2. Your dashboard will show the alerts you have subscribed to.
3. Use the filter bar to apply filters such as **TLP, Category, Published Date, Source, Priority,** and more.
4. Select the alert card to view its details.
5. From an alert, you can:
    a. Create Actions
    b. **Export** the alert for offline analysis

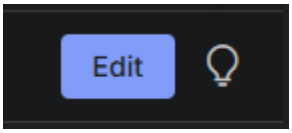
Alert Notifications (Email & SMS)

The **alert notifications setting** controls email and mobile notifications for each alert category.

6. Sign in to the TX-ISAO Portal.
7. Go to **Settings** by selecting the gear icon in the bottom left corner of the screen.



8. Select the **Edit button** in the top right corner of the screen.



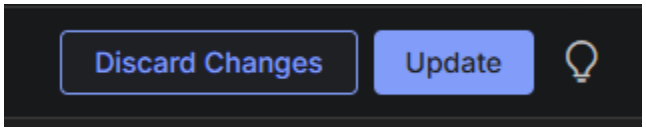
9. For **Admin Enabled Categories**, select or deselect the **Email** and/or **Mobile** checkboxes for each category.

Note: Admin enabled categories cannot be fully disabled, but you can turn off their email/mobile notifications (the alert will still show on your member dashboard).

10. For **Optional Categories,** use the toggle to enable/disable the category entirely, then select your preferred Email and/or Mobile notification checkboxes.

Note: If you disable the Alert toggle, you will no longer receive notifications for this category nor will you be able to view that category's alert on your member dashboard.

11. Click **Update** at the top right corner of the screen or select **Discard Changes**.



Share Threat Intel

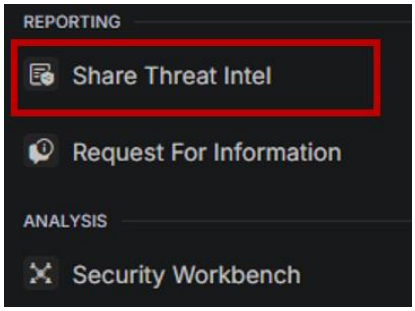
The **Share Threat Intel** feature allows members to share cybersecurity threat intelligence directly with analysts. The intel helps analysts evaluate and understand an organization's most frequent or severe external risks and threats, which can then be shared as alerts to the broader member community.

Disclaimer: *Do not include any identifiable information or attribution. This form should only be used for sharing obfuscated threat indicators/observables (e.g. IP, URL, Filename, Hash, Domain Name).*

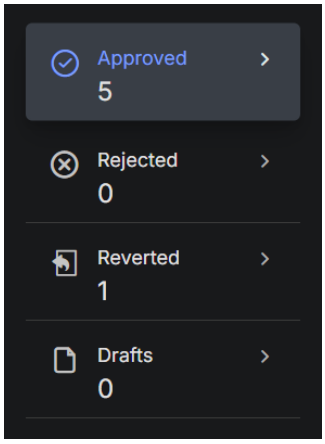
1. Sign in to the TX-ISAO Portal.
2. Select the three horizontal lines in the top left corner of the screen.



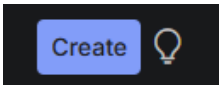
3. Under Reporting, select the **Share Threat Intel** option.



4. From this page, you will be able to view your previous submissions (if any) and the status of each.



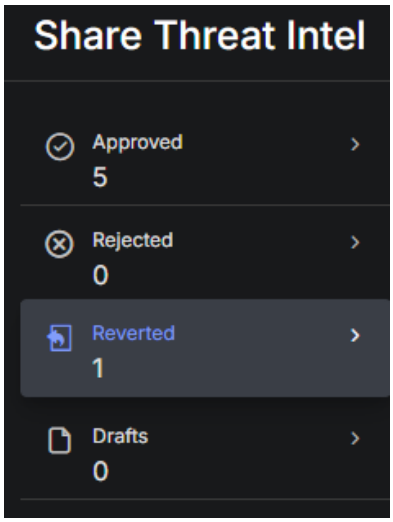
5. Select **Create** in the top right corner of the screen.

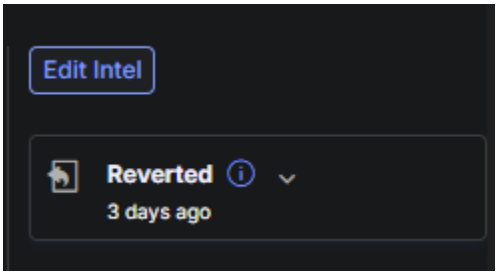


6. Select the **Category** that best fits the intel you want to submit.
    a. **GRC Hub** – Select this category if you want to submit a document to the GRC Hub. For more information, see the GRC Hub section of this document.
    b. **Threat Intelligence** – Select this category for all other cybersecurity threat intelligence.
7. Complete the **required** submission fields.
8. TXCC automatically anonymizes threat intel submissions. If you want to share your identity, select **Would you like to provide attribution for this form?** at the bottom of the **Basic Details** section.

Note: Privileged analysts may still access your identity even if you do not select this box.

9. **Preview** your submission. If you need more time before submitting, select the **Save as Draft button** at the bottom of the screen. **Important:** After you submit, you will not be able to edit the submission unless an analyst reverts the submission.
10. When you are ready to submit your intel, select **Submit** at the bottom of the screen.
11. Once submitted, an analyst reviews your submission before approving, reverting, or denying it.
12. You will receive an email and an in-app notification when your submission status changes.
13. If **reverted**, the analyst will provide a comment for more information.
14. You will be able to view the analyst's comment and edit the intel by navigating to the **Reverted** option and selecting the **Edit Intel button**.





15. Make the necessary revisions requested by the analyst, then re-submit the intel.

Request for Information

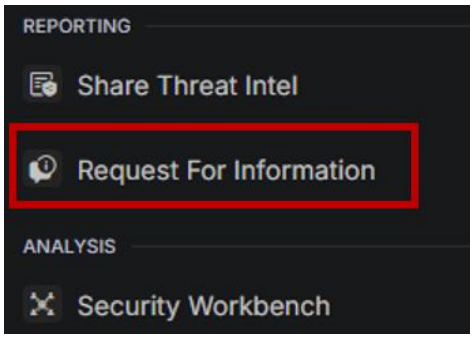
The **Request for Information (RFI)** feature is a formal process for members to gather relevant and contextual information on cybersecurity threats, vulnerabilities, malware, threat actors, or incidents to support security decision-making.

Disclaimer: *Do not submit any personally identifiable information, including credit card or bank account information; social security, passport, or driver's license number; date of birth; account PINs, passwords or any other sensitive information in the report. This form should be used for requesting information that may be related to physical or cyber security.*

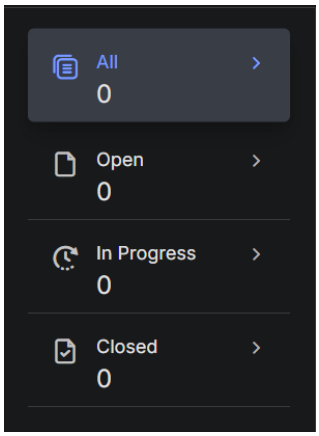
1. Sign in to the TX-ISAO Portal.
2. Select the **three horizontal lines** in the top left corner of the screen.



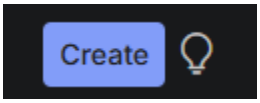
3. Select the Request For Information option.



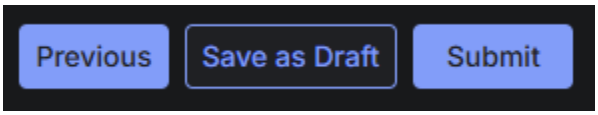
4. From this page, you can **view your previous submissions** (if any) and the **status** of each.



5. Select **Create** in the top right corner of the screen.



6. Fill in the **required** request fields.
7. **Preview** your request. If you need more time before submitting, select the **Save as Draft** button at the bottom of the screen. **Important:** After you submit, you will not be able to edit the request.
8. Once ready to submit your RFI, select the **Submit** button at the bottom of the screen.



9. Once submitted, your RFI is sent to an a**nalyst for review**. You will receive:
    a. An **email and an in-app notification** confirming that you submitted an RFI and another notification when your RFI moves to **In Progress**.
    b. A notification when the RFI is **Closed** that includes a closing comment visible to you.
10. Analysts may also create an alert directly from your RFI.

Events

The **Events** feature allows members to view events, such as the TX-ISAO Monthly Meeting and TXCC's Monthly Security Meeting. Members are also able to submit event requests for cybersecurity-related events, such as summits, expert webinar series, meetings, and conferences.

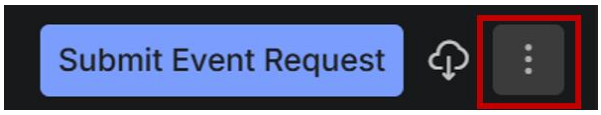
Accessing Events

To access the **Event feature**:

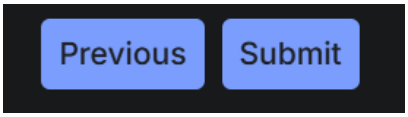
1. Sign in to the TX-ISAO Portal.
2. Select the **clock icon** in the bottom left corner of the screen.



3. From this screen, you can see a calendar view of the current month and any cyber-related events submitted through the TX-ISAO. You can also view a list of upcoming events to the left of the calendar.
4. To submit an event request, select the **Submit Event Request button** at the top-right corner of the screen.



5. Fill in the required request fields.
6. In the **Event Schedule section**, include the following information:
    a. Time Zone
    b. Event Date
    c. Event Start and End Time
    d. Place or Address of Event
    e. Event URL (if applicable)
7. Preview your request, then select **Submit** at the bottom of the screen.



TXCC Monthly Meetings

TXCC hosts two different meetings each month:

1. TX-ISAO Monthly Meeting (**TLP: GREEN**):
    a. This meeting brings together cybersecurity professionals from across Texas to share the latest information on threat intelligence, security trends, and statewide cyber initiatives.
    b. This meeting is open to all TX-ISAO members.
    c. Meetings are held on the third Tuesday of each month from 9:00 A.M. to 10:30 A.M. CST.
2. Monthly Security Meeting (**TLP: AMBER**):
    a. TXCC hosts a monthly security meeting for security leaders from state agencies and institutions of higher education. The meeting includes relevant statewide updates, highlights from TXCC Cybersecurity Operations, GRC, and Security Services, as well as a monthly tabletop exercise.
    b. This meeting is only available to State Agency and Institutes of Higher Education (IHE) members.
    c. Meetings are held on the second Thursday of each month from 9:00 A.M. to 10:00 A.M. CST.

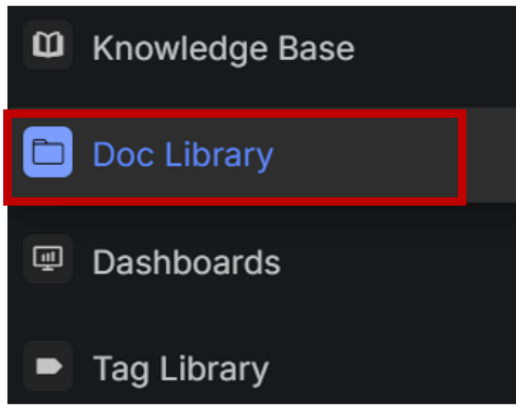
TXCC schedules all meetings for the Fiscal Year. The meetings can be accessed via the Events feature of the portal with the link available to join each meeting.

After each monthly meeting, an analyst will upload the meeting's presentation to the TX-ISAO Portal. **To access past meeting presentations:**

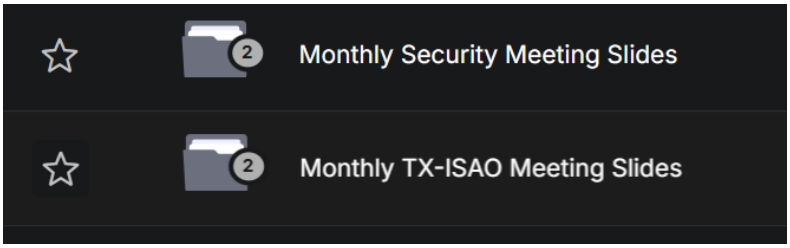
1. Select the three horizontal lines in the top left corner of the screen.



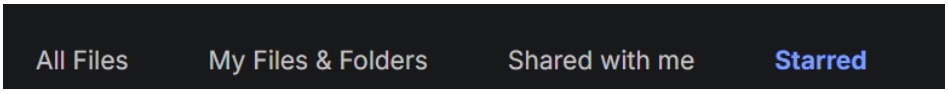
2. Select the **Doc Library** option.



3. Locate the meeting folder you want to view and navigate to the version you want to access.



4. If you select the **Star button**, that folder will appear in the **Starred** option at the top of the page for easy access.



Note: If you have access to a monthly meeting but do NOT have access to the corresponding Doc Library folder, contact TX-ISAO@txcc.texas.gov.

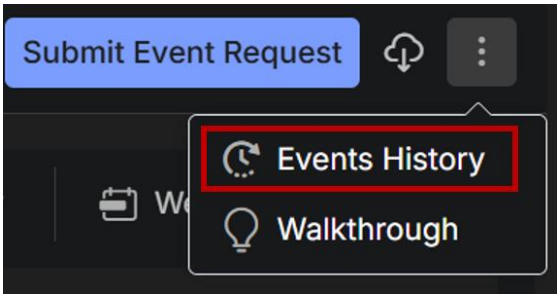
View Past Event Submissions

To view your past Event submissions and their status:

1. Sign in to the TX-ISAO Portal.
2. Select the **clock icon** in the bottom left corner of the screen.



3. Select the three vertical dots icon next to Submit Event Request, then select **Events History**.



4. From this page, you can view your previous submissions and their statuses.

GRC Hub

The **Governance, Risk, and Compliance (GRC) Hub** is a centralized repository that enables TX-ISAO members to share samples or templates of GRC documents. GRC documents include foundational policies, procedures, standards, and other documents used by an organization to manage its GRC activities. By leveraging resources shared by TX-ISAO members, organizations can improve their GRC practices, align with industry standards, and address common regulatory requirements more efficiently.

Accessing the GRC Hub

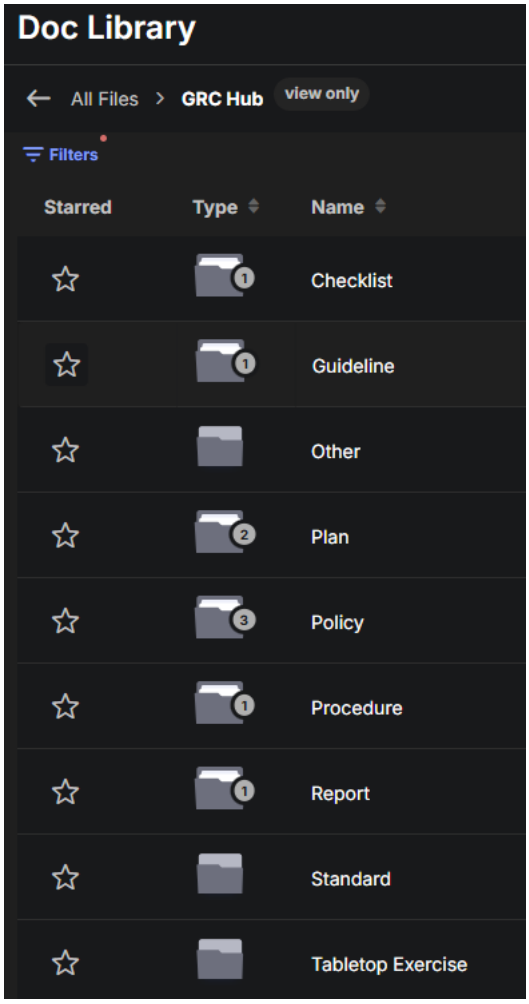
To access the **GRC Hub**:

1. Sign in to the TX-ISAO Portal.

2. Select the three horizontal lines in the top left corner of the screen.



3. Select the **Doc Library** option.
4. Open the GRC Hub folder.
5. Open the folder with the **document type** that you want to locate.
6. To search for a document format, select **Filters** and then **Tags**. Then, search for **Format:** to find a document by format, such as Example or Template. You can also use Tags to search for a specific tag, such as **Incident Response**.



Note: If you do NOT have access to the GRC Hub folder, contact TX-ISAO@txcc.texas.gov.

GRC Hub Submissions

Members can submit documents for inclusion to the GRC Hub. By leveraging resources shared by TX-ISAO members, organizations can improve their GRC practices, align with industry standards, and address common regulatory requirements more efficiently.

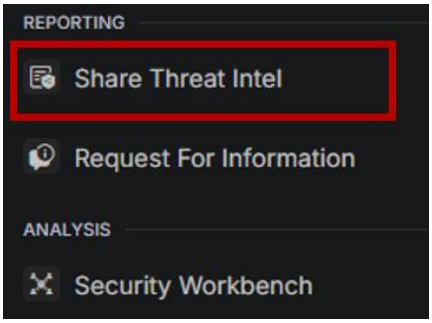
Disclaimer: *Individuals contributing documents to the GRC Hub should only share documents that they are authorized to share. Contributors are responsible for ensuring that documents are appropriately redacted before submission.*

To submit a document to the GRC Hub:

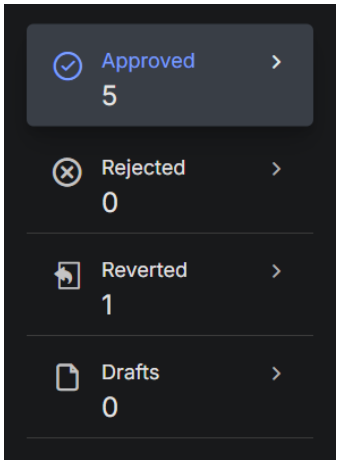
1. Sign in to the TX-ISAO Portal.
2. Select the three horizontal lines in the top left corner of the screen.



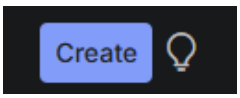
3. Select the **Share Threat Intel** option.



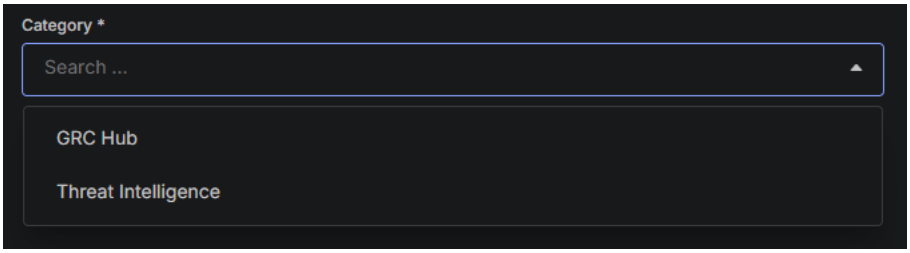
4. From this page, you will be able to view your previous submissions (if any) and the status of each.



5. Select **Create** in the top right corner of the screen.



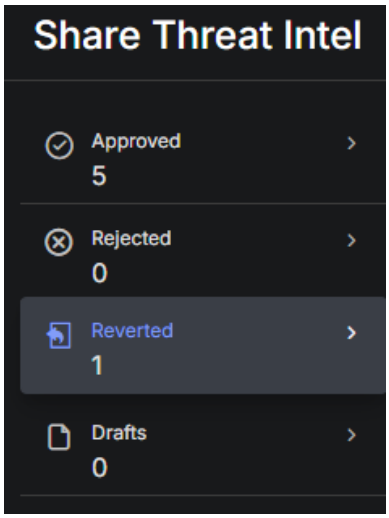
6. Select **the GRC Hub Category**.

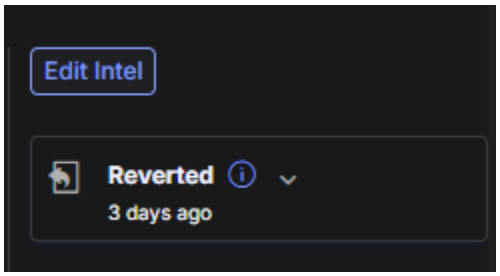


7. Complete the **required** fields, select any applicable tags (optional), and **attach your PDF document** to the **Attachments** section.
8. TXCC automatically anonymizes threat intel submissions. If you want to share your identity, select the **Would you like to provide attribution for this form? button** at the bottom of the **Basic Details** section.

Note: Privileged analysts may still access your identity even if you do not select this box.

9. **Preview** your submission; if you need more time before submitting, select the **Save as Draft button** at the bottom of the screen. Once submitted, you will not be able to edit the submission unless an analyst reverts the submission.
10. Once ready to submit your document, select the **Submit button** at the bottom of the screen.
11. Once submitted, an analyst will review your submission before **approving, reverting,** or **denying** it.
12. You will receive an email and an in-app notification when your submission moves to a new status.
13. If **reverted**, the analyst will provide a comment for more information.
14. You will be able to view the analyst's comment and edit the intel by selecting the **Reverted** option and selecting the **Edit Intel button**.





15. Make the necessary revisions requested by the analyst before re-submitting.
16. Once approved, an analyst will add your document to the GRC Hub folder.

Traffic Light Protocol

The Traffic Light Protocol (TLP) facilitates easier sharing of information. TLP is a set of "classifications" used to describe with whom sensitive information can be shared. TLP has four color designations and one color + modifier designation:

1. **TLP: RED** - Not for disclosure; restricted to participants only
2. **TLP: AMBER + STRICT** - Limited disclosure; restricted to participants' organizations
3. **TLP: AMBER** - Limited disclosure; restricted to participants' organizations or clients
4. **TLP: GREEN** - Limited disclosure; restricted to the community
5. **TLP: CLEAR** - Disclosure is not limited

Need Help

Please email TX-ISAO@txcc.texas.gov for all questions or concerns.