USER

MANUAL

California Compliance and Security Incident Reporting System (Cal-CSIRS), ***Incident Reporting Module***

California Information Security Office and
The California Highway Patrol

October 2nd, 2022

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	03/24/2016	User Manual Template Downloaded from U.S. HUD
Rev. 1; v2.0	04/05/2016	Template modified and first draft created
Rev. 2; v3.0	04/18/2016	First review/revision by internal staff
Rev. 3; v4.0	06/16/2016	First update for Cal-CSIRS Launch
Rev. 3, v5.0	09/08/2016	Second update since Cal-CSIRS Launch
Rev. 7, v7.0	10/16/2020	SOC SEN Update & Formatting
Rev. 8, v 8	04/25/2022	Fraudulent Activity Incident Type
Rev 9, v 9.0	09/28/2022	Addition of Risk Mitigated Response Type (Low) process and its associated incident response time frame & update to the False Positive process.

USER MANUAL

TABLE OF CONTENTS

Page

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

1.1 System Overview

The California Compliance and Security Incident Reporting System (Cal-CSIRS) is the state's single source application for reporting, tracking, analyzing, and resolving Information Security incidents. The Cal-CSIRS is not a case management system and should not be considered the only repository of information related to California's security incidents. Although the system and data it contains are categorized as Moderate on the FIPS-199 potential impact spectrum, the system is not designed to store or process criminal or attorney-client privileged information. System users shall use due care when entering data and shall only input information based on need-to-know principles.

The California Information Security Office (CISO) is the system and data owner, with special privileges granted to authorized individuals at the California Highway Patrol (CHP) and the Governor's Office of Emergency Services (CalOES). Changes and updates shall be managed by the CISO.

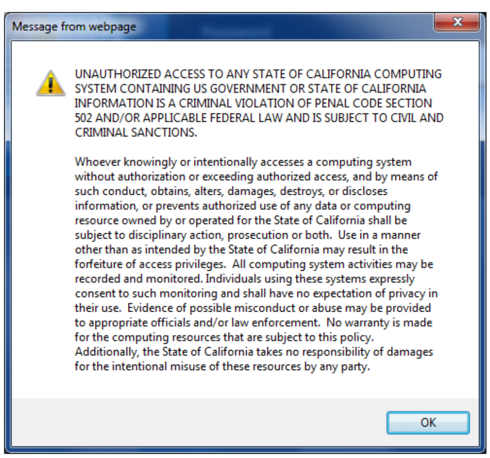
1.2 Project References

References used in preparation of this document include:

- Rsam 2016 Customer Guide
- Rsam Incident Management Walkthrough Guide for the State of CA
- Rsam Version 9 Release Notes
- Cal-CSIRS development instance

1.3 Authorized Use Permission

Users of this system agree to the terms and conditions as described in the warning banner shown during each logon attempt.



Questions regarding access controls shall be directed to:

California Department of Technology (CDT)
California Information Security Office (CISO)
PO Box 1810; MS Y-12
Rancho Cordova, CA 95741
security@state.ca.gov
(916) 445-5239

1.5 Organization of the Manual

This manual is organized by the following major sections:

General Information	A high-level system overview is provided with a couple of caveats that help manage users' expectations.
System Summary	This section contains simple information describing system configurations, data flows, access levels, and contingency planning. This section is intentionally non-technical.
Getting Started	This is where the user will learn basic information related to accessing and exiting the system.
Using the System	This section contains detailed instructions for proper use of the system. Much of the system instructions are displayed on system screens in the form of tooltips, dropdowns, and field-level labels. The system was designed to allow for rapid input of basic incident information. This will allow the user to enter the basics, and then return to managing the people and technology related to the incident. Furthermore, the basic information during the initial input phase will provide other users (CHP, CISO, and others) an awareness of the incident and a sense of its criticality.
Searching	To enhance usability, the system contains searching and querying capabilities. This section will explain those capabilities.
Reporting	Cal-CSIRS' reporting capabilities is an important feature, second only to situational awareness. This section will instruct and illustrate the basic reporting capabilities. For more detailed searching and reporting capabilities, contact the system owner – CISO.

1.6 Acronyms and Abbreviations

Cal-CSIRS ....California Compliance and Security Incident Reporting System
CalOES ....California Office of Emergency Services
CCIU..Computer Crimes Investigation Unit (CHP)
CDT ....California Department of Technology
CHP..California Highway Patrol
CIO...Chief Information Officer
CISO ....California Information Security Office
CISO ....Chief Information Security Officer
ENTAC ....Emergency Notification Tactical Alert Center (CHP)
RDMS ....Relational Database Management System
SaaS ....Software as a Service

2.0 SYSTEM SUMMARY

2.0 SYSTEM SUMMARY

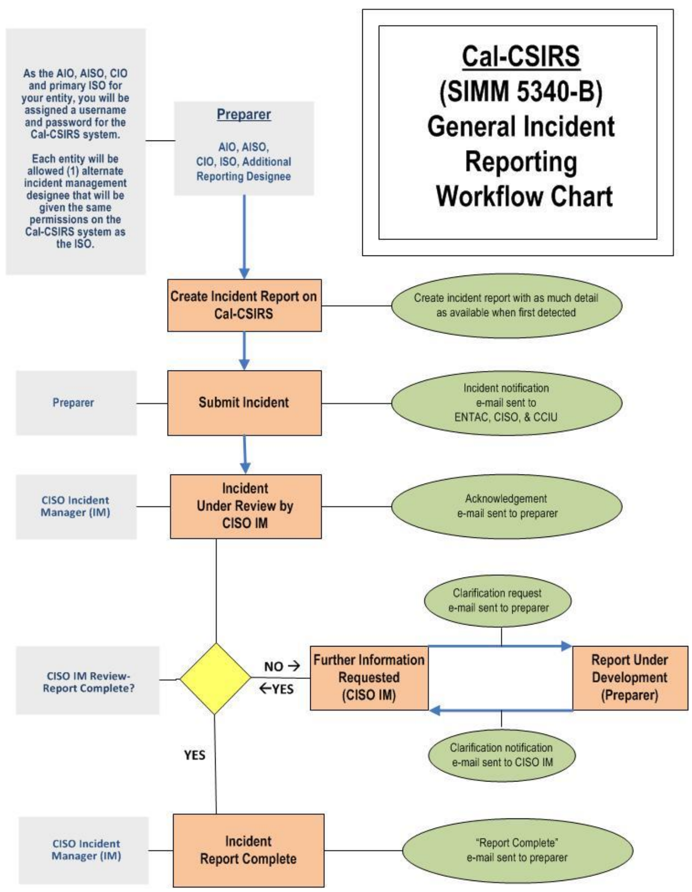
The Cal-CSIRS is a Relational Database Management System (RDBS) with a user-friendly interface and incorporates a workflow engine, robust reporting capabilities, and business rules that guide the user.

2.1 System Configuration

The Cal-CSIRS is a Software-as-a-Service (SaaS) application hosted in the Cloud. Hardware, software, and networks are maintained by the vendor according to CISO's specifications.

2.2 Data Flows

Once a user creates an incident it is acknowledged by the California Information Security Office. Users may continue to add additional reporting detail, upload requested or required documents and complete all relevant questions during the investigation period using the "Save and Close" button after making each additional entry. When a user believes they have provided all necessary information, by completing all necessary fields they can request that the incident be closed by using the "Final Update" button. The diagram below is the source of most business rules and decision points embedded in Cal-CSIRS. If the workflow is not clear, the CISO can provide further information.



2.3 User Access Levels

There are several specific roles applied to users and objects in the system. Users may possess one or more of the following roles:

CISO ....Access[1] to all incident records
Agency..................Access to records assigned to the agency and all subordinate departments
Department............Access to records assigned to the specific department

2.4 Contingencies and Alternate Modes of Operation

The Cal-CSIRS shall be available 24/7 from predetermined end points using authorized credentials. The Cloud-based SaaS is hosted at a west coast data center and replicated in geographically disparate locations to ensure availability in the event of a regional disaster.

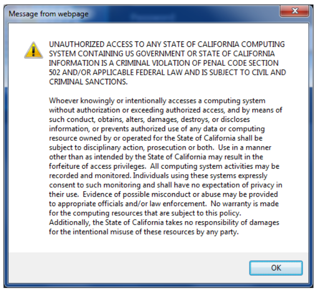
[1] In this context "Access" is defined as the ability to create, view, update, and/or close an incident record.

3.0 GETTING STARTED

3.0 GETTING STARTED

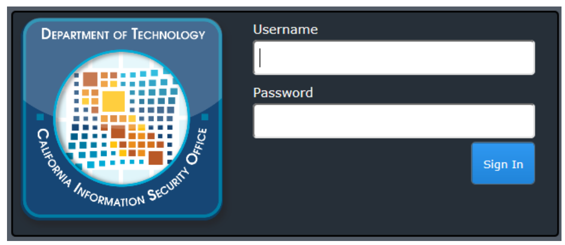
3.1 Logging On

1. Using your browser, navigate to: https://calcsirs.rsam.com/ . You will be presented with a logon banner.

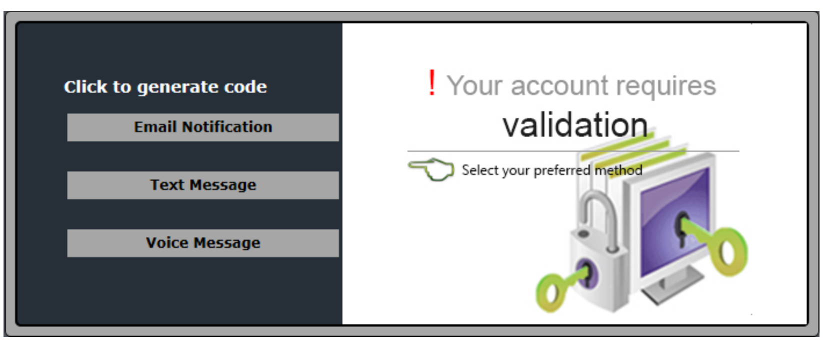


2. Click OK to continue after reading the message.

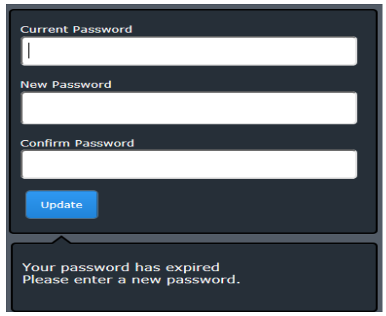
3. Sign in with your Username and Password



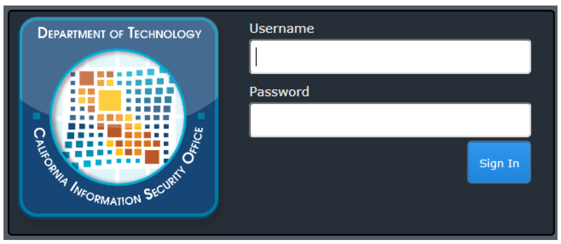
4. You will next be asked to select the communication method you wish to receive your second factor authentication. Note: If you did not proved a cell phone number you will not be able to use the text message option. You will receive a onetime use PIN via that selected method. Once you receive your PIN, enter it into the next popup screen.



5. If this is your first logon, you will be prompted to change your Password. Enter Current Password then enter your New Password and enter again to Confirm New Password

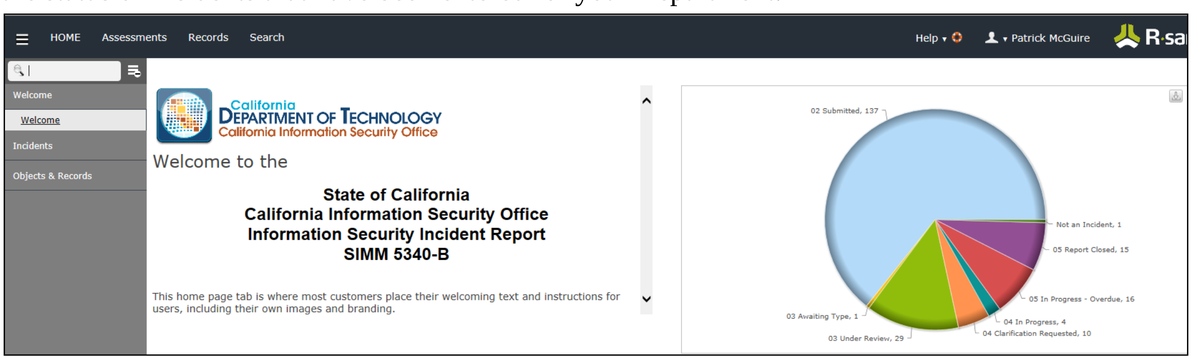


6. Log in with your New Password



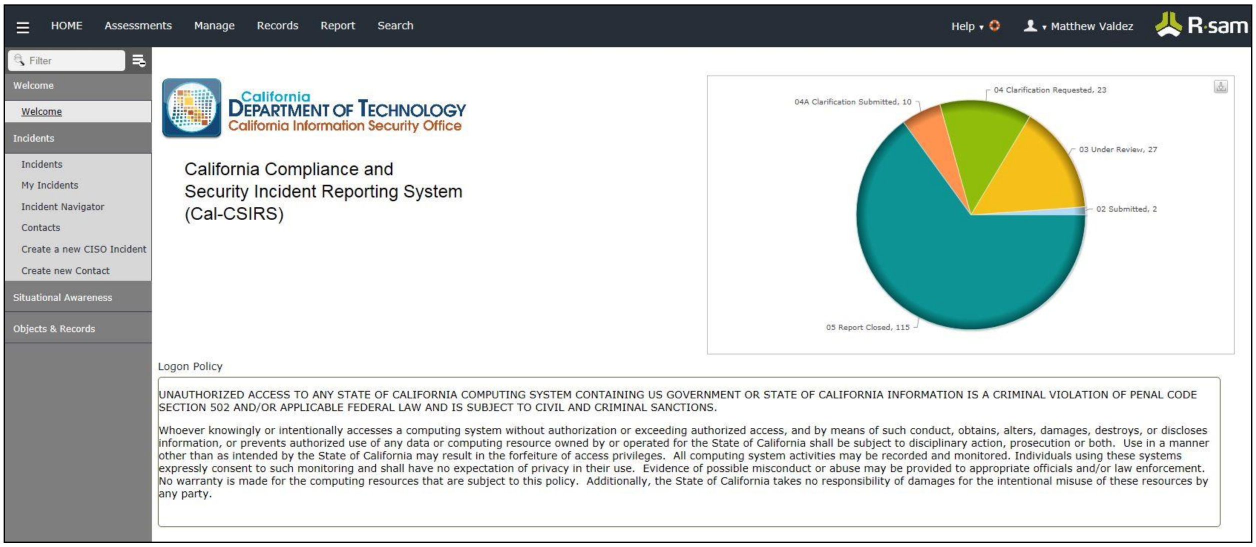
3.2 System Menu

1. The Welcome Screen is your first system landing page where you can view data (see pie chart) on the status of incidents that have been entered for your Department.



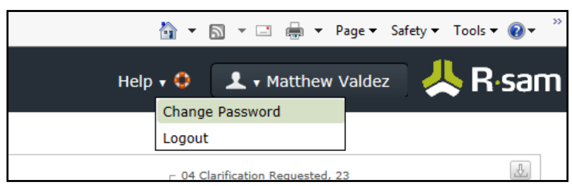
2. Click "Incidents" in the left navigation pane, this will display your options

3. The Incidents page displays graphs of Incidents by Workflow State, All Types, and Significance.



3.3 Changing User ID and Password

Your user ID is established by the CISO and not subject to change. Each user must have his or her own ID and you should never share an ID or password with anyone else. If you need additional User IDs for your department, please contact the CISO. You can, however, change your password at will. At the top of most screens is a static black banner. Your user ID is toward the right side of the screen. When you move your mouse over your user ID you will be given two options: 1) change password; and 2) logout. When selecting “change password”, you will be provided a self-explanatory window for password changes.



3.4 Exit System

To exit the system, use option #2 (see the above paragraph - Section 3.3). You will be prompted to save your work if you’ve not already done so.

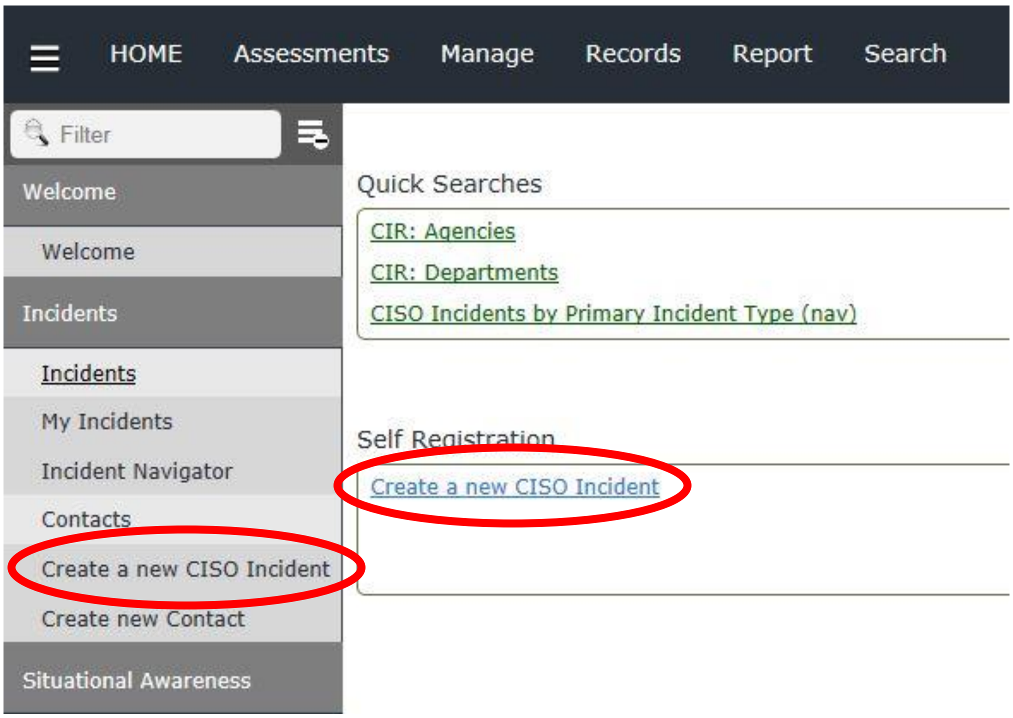
If you are accessing this application from a non-state owned device, please delete all temporary files and history.

4.0 USING THE SYSTEM (ONLINE)

4.0 USING THE SYSTEM (ONLINE)

4.1 Initial Input – Creating a new CISO Incident

1. To create a new incident select ***Create a new CISO Incident***, in either of the two locations circled below.

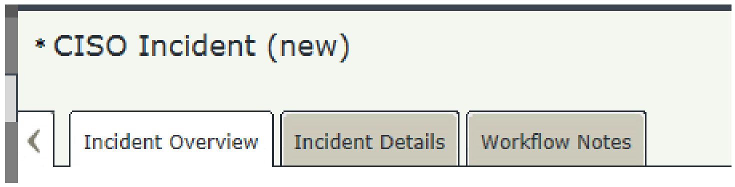


2. The next screen is a list of departments. Click ***Select*** under the Category heading to select the department/entity for your reporting. In most cases, there will only be one entity to select. When you ***Select*** the department, you will be taken to the Incident screens.

Select from the list below

Name	Type	Entity	State	Category
▽	▽	▽	▽	
ABC	Department	Information Security Office	N/A	Select
abcappealsbd	Department	Information Security Office	N/A	Select
BCSH	Agency	Information Security Office	N/A	Select

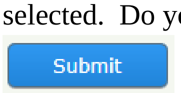
3. The Incident screens are divided into three tabs:
   - ***Incident Overview*** tab is for incident contact information, description, corrective actions, incident cost details, and file uploads.
   - ***Incident Details*** tab is where the Incident Type(s) will be selected and the characteristics of the incident are requested.
   - ***Workflow Notes*** where you will find the Incident Report due date and comments from the incident manager during the incident reporting process.

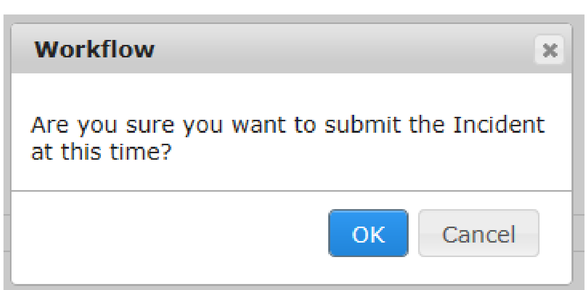


4. In the Incident Overview tab enter mandatory information into the fields marked with a red asterisk *. If you have additional information about the incident at this time, complete those other fields.

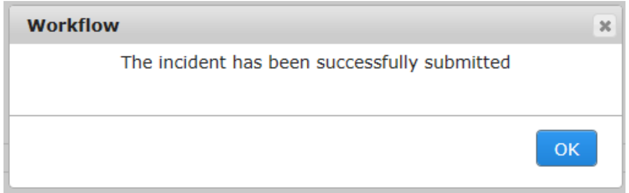
> **Important Note:** There are 7 fields you **must** complete prior to submitting the incident (6 on the "Incident Overview" tab and 1 on the "Incident Details" tab). This was by design. If this incident is unfolding in real time and it needs your immediate attention, you can submit the incident with the 7 required data elements and return to entering additional information later. Once you have entered information in all red asterisk * fields and clicked on "Submit", the workflow will notify your external partners. Based on the incident email and whether you selected "Yes" to the question ***"Is this a Significant Incident"***, external partners may contact you to discuss mobilizing resources.

5. Next, click the Incident Details tab and select a Primary Incident Type by using the drop down. This is a mandatory field. If there is a secondary Incident Type known at this time, select Additional Incident Type. You will be prompted to provide additional information based on the Incident Type(s) selected. Do your best to complete the information and then click Submit at the top of the screen.





If all the mandatory fields are complete you will be asked to confirm, click OK to submit the Incident to the CISO. Cal-CSIRS workflow then will display a confirmation message.



Click OK to clear the confirmation message.

You have now completed the initial input stage. The system will return to the Incident Navigator view, where you can click My Incidents to display Incidents by Workflow State.

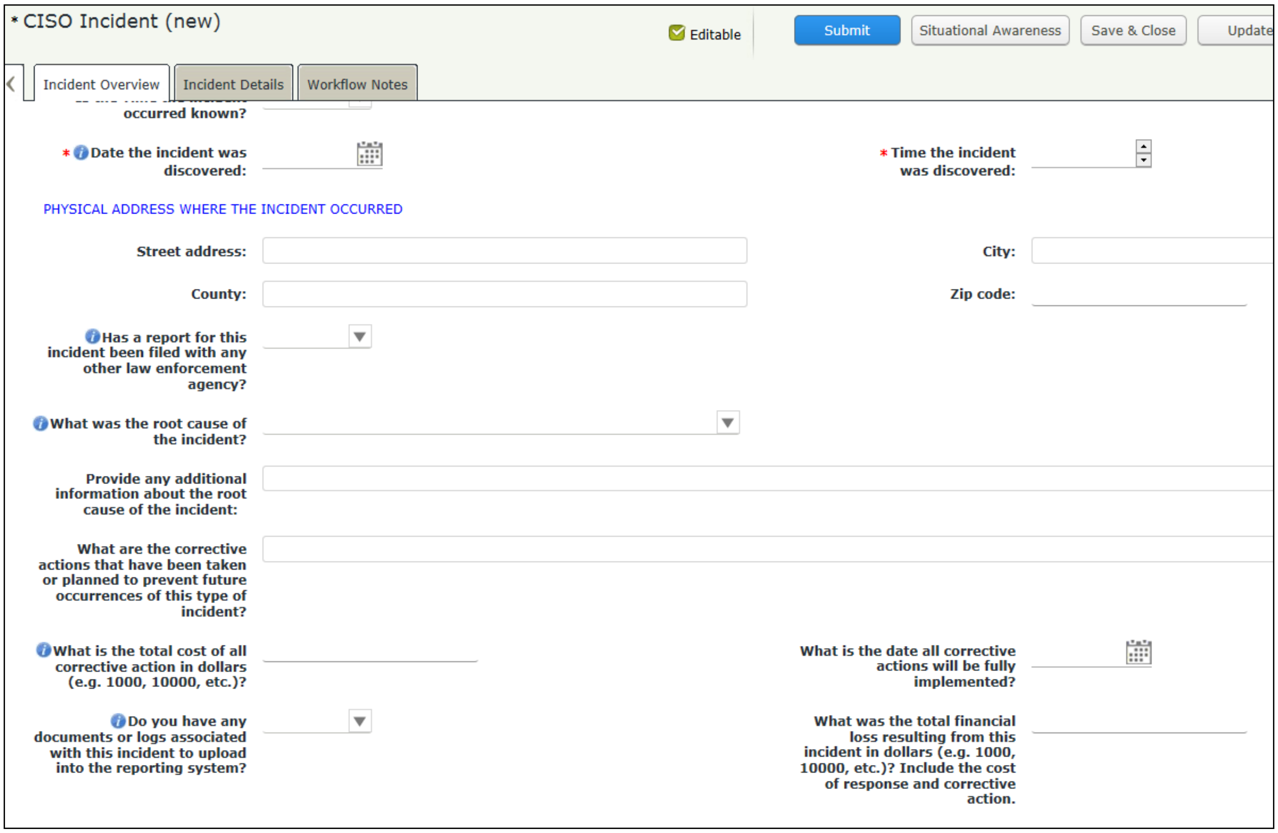
Additionally, the system will send an acknowledgement email (RSAM Notification example below) and will also send an email to the CISO, ENTAC, and to CCIU.

4.1.1 Incident Overview Tab

As a user of the Cal-CSIRS, you will find most of the instructions are provided in the application screens through the use of 1) tooltips; 2) dropdown fields; 3) verbose labels; and 4) search icons that display a selection menu. This user manual will get you started and allow the online instructions to guide you.

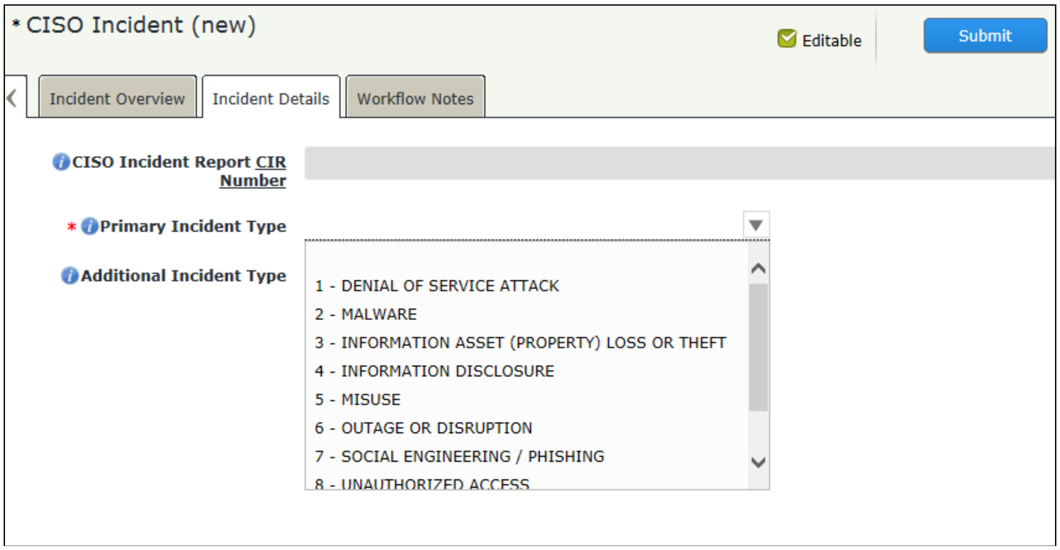
The following screen shot shows the very bottom of the Incident Overview tab. At this location, the incident preparer can provide:

- Root Cause of the incident
- Corrective Actions taken (or planned) to prevent future, similar incidents
- Total Cost of Corrective Actions
- Total Financial Loss to the State, which includes the Total Cost of Corrective Actions
- File Uploads, relevant to this incident.



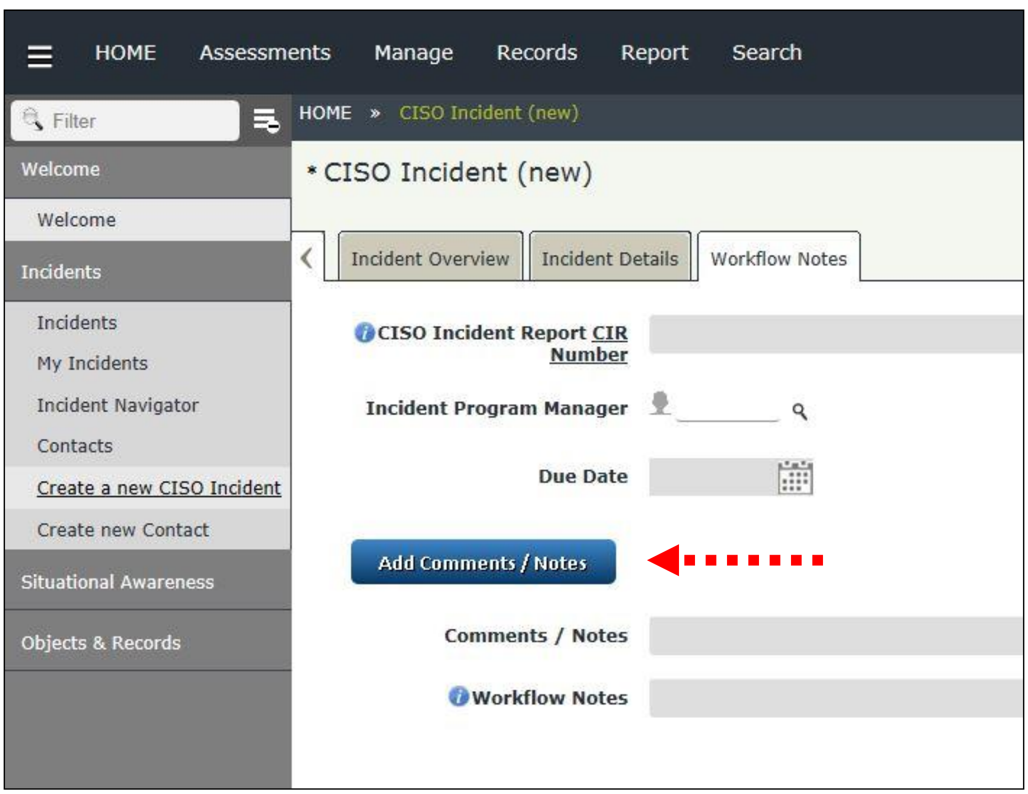
4.1.2 Incident Details Tab

The Incident Details tab is where the user enters the specific information related to the incident. The first selection, "Primary Incident Type", may have been selected during the rapid initial input. Depending on which incident type you select, the system will display a series of input fields which are applicable to that incident type. It is important to complete as many fields as possible, otherwise the CISO or CHP may need to contact you for supplemental information.



4.1.3 Workflow Notes Tab

The Incident Details tab is where the user can communicate messages to CISO and CHP. The messages are date/time stamped, and Cal-CSIRS will save the notes as an archive, regarding the communication and deliverables for the incident.

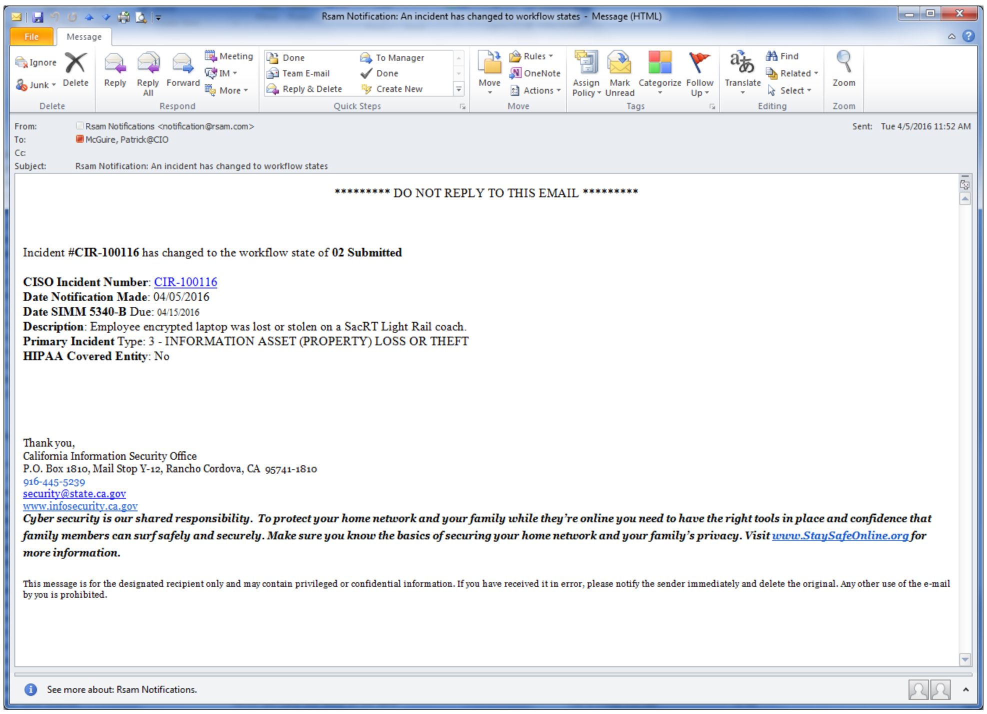


4.2 Email Notifications

The Cal-CSIRS incident will move through the different workflow states:

- Draft
- Submitted
- Under Review
- Clarification Requested
- Clarification Submitted

As the incident changes workflow states, auto-generated emails will be sent either to the user/preparer or to the CISO office. The message provide a summary detail of the incident and the status. The emails will alert the user that an incident is waiting for review or response. The emails can also be forwarded as "incident updates" to managers and to those who have an interest in the status of specific incidents. The email below is presented as a sample.



Rsam Notification: An incident has changed to workflow states - Message (HTML)

From: Rsam Notifications <notification@rsam.com>
Sent: Tue 4/5/2016 11:52 AM
To: McGuire, Patrick@CIO
Cc:
Subject: Rsam Notification: An incident has changed to workflow states

********* DO NOT REPLY TO THIS EMAIL *********

Incident **#CIR-100116** has changed to the workflow state of **02 Submitted**

CISO Incident Number: CIR-100116
Date Notification Made: 04/05/2016
Date SIMM 5340-B Due: 04/15/2016
Description: Employee encrypted laptop was lost or stolen on a SacRT Light Rail coach.
Primary Incident Type: 3 - INFORMATION ASSET (PROPERTY) LOSS OR THEFT
HIPAA Covered Entity: No

Thank you,
California Information Security Office
P.O. Box 1810, Mail Stop Y-12, Rancho Cordova, CA 95741-1810
916-445-5239
security@state.ca.gov
www.infosecurity.ca.gov
Cyber security is our shared responsibility. To protect your home network and your family while they're online you need to have the right tools in place and confidence that family members can surf safely and securely. Make sure you know the basics of securing your home network and your family's privacy. Visit www.StaySafeOnline.org for more information.

This message is for the designated recipient only and may contain privileged or confidential information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the e-mail by you is prohibited.

See more about: Rsam Notifications.

4.3 Special Instructions for Error Correction

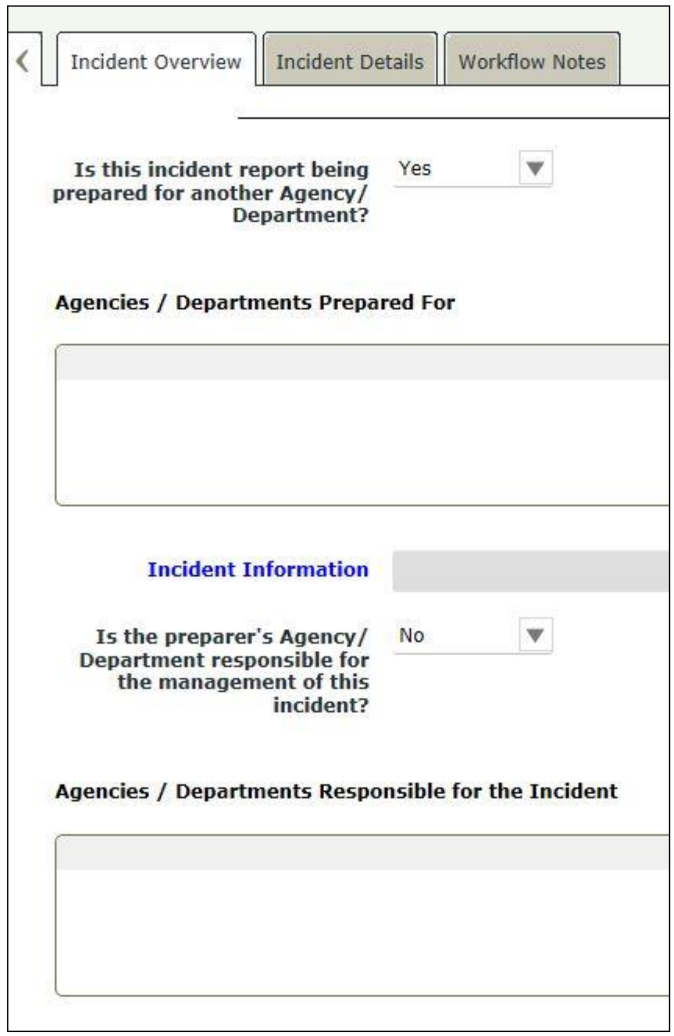
If during use of Cal-CSIRS you receive an error or you find you are not able to perform a required action, please contact the CISO. Details and screen prints will be helpful.

4.4 Uploading Files - Breach Notification Letter, Log Files, Etc.

On occasion it may necessary to upload multiple, relevant files into the Cal-CSIRS incident report. As examples only, the user may need to upload Log Files or a Breach Notification for review. This is done by at the bottom of the Incident Overview tab. Please note that you will still need to contact CISO by telephone to let them know when a Breach Notification has been uploaded for review and approval. Also DO NOT attempt to upload malware or malicious files into Cal-CSIRS..

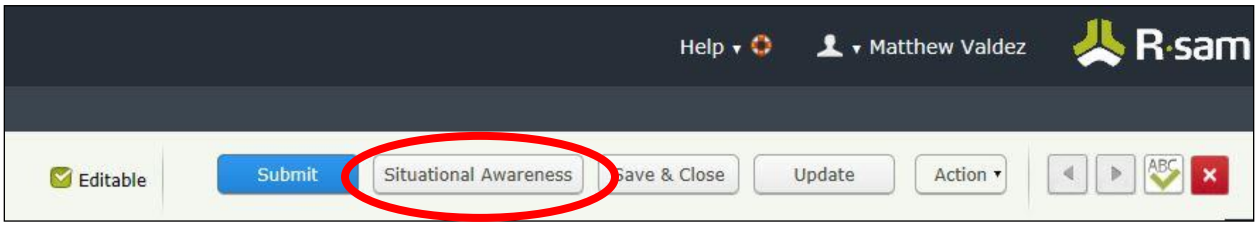
4.5 Open an Incident on behalf of another department

On occasion it may necessary to log an incident on behalf of another department. This can be a common practice if the "backup ISO" is covering another department or if the ISO has prevue over more than one department. In the Incident Overview tab (middle), a question asks, "Is this report being prepared for another Agency/Department?" When the user inputs "Yes", then a pulldown appears for the user to identify the department. The following question asks, "Is the preparer's Agency/Department responsible for the management of this incident?" Depending on the response, additional fields will appear to allow for clarification of the incident owner.



4.6 Situational Awareness Report (SAR)

A situational awareness report (SAR) allows users to broadcast a situational awareness. The situational awareness report allows a user to share information, to all Cal-CSIRS users, about anomalous or suspicious activity they've observed that has not risen to a reportable incident for their entity. As an example, a large department may wish to share that it is seeing an unusually high volume of traffic from a specific IP or IP range. The situation may not have resulted in an outage or disruption but could impact others and would be worth sharing. To create a Situational Awareness Report use the "Situational Awareness" button instead of the "Submit" button. Please also note (1) that a "Situational Awareness" is not yet a submitted incident and (2) that only CISO and "creator" will be able to edit a Situational Awareness



5.0 SEARCHING

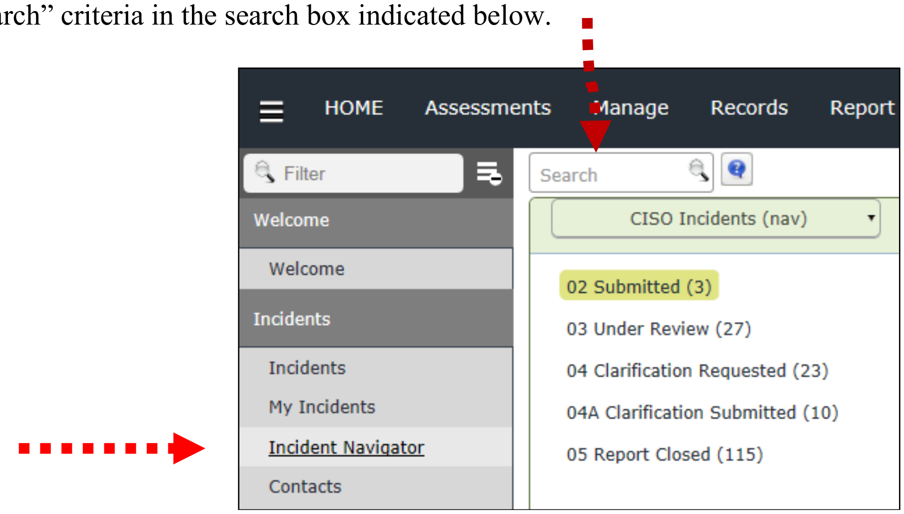
5.0 SEARCHING

5.1 Search Capabilities

The Cal-CSIRS limits the search capabilities for users. Users can execute Existing Searches and create new searches within the users' assigned data stores. If you need additional search capabilities, please contact the CISO.

5.2 Standard Search

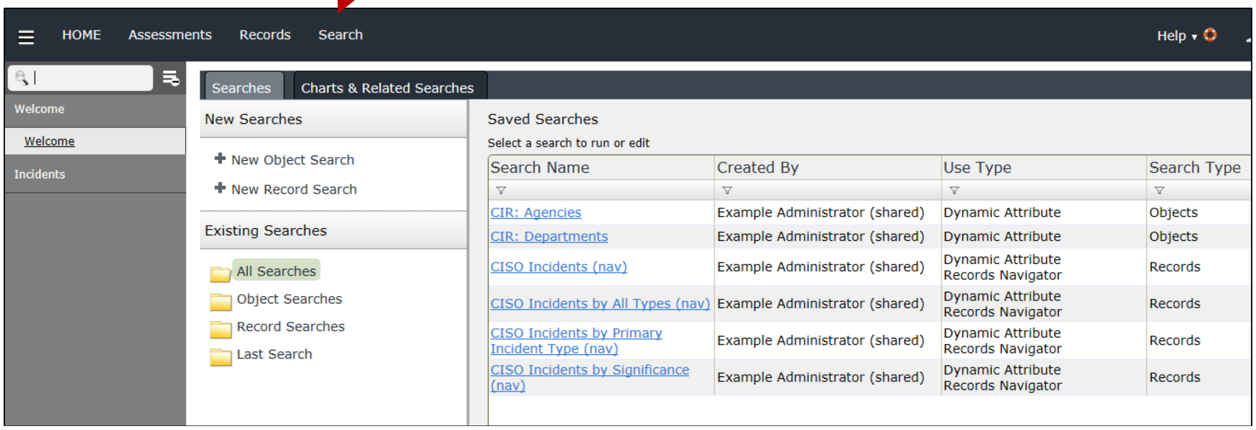
To perform a standard search for an incident, first open the "Incident Navigator" tab and then input the "Search" criteria in the search box indicated below.



Once the search is complete, be sure the clear the search by selecting the white "x" in the red box, next to the search box.

5.3 Advanced Search Procedures

To perform an advanced search, select "Search" located in the main menu at the top of the screen. You will then be presented with a screen similar to the one below.



At this point, you may select one of the saved searches provided or create a new one. Unless you have been trained on creating search criteria, it is recommended you only access existing searches.

6.0 REPORTS

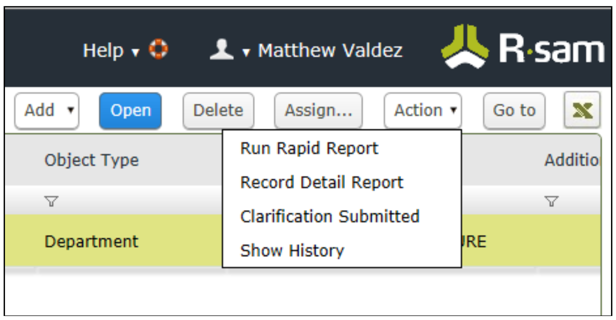
6.0 REPORTS

6.1 Report Capabilities

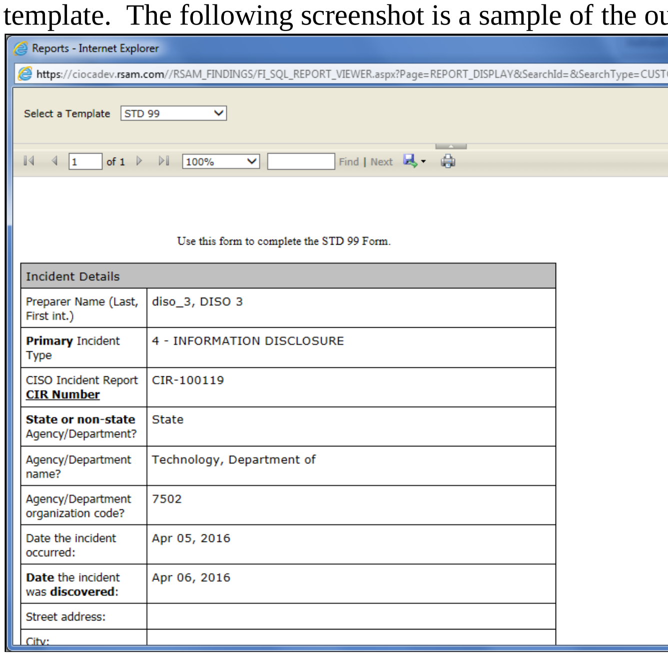
Cal-CSIRS reporting capabilities allow users to report the details of a single incident. The user can also export a block of incidents for an incident group report by date or by incident type. Reporting will be expanded even more in the next release. In addition to traditional reports showing specific data elements, Cal-CSIRS can also generate charts of various types – bar, pie, 3D, etc.

6.2 Single Incident Report Procedures

With the “Incident Navigator” open, the user can select (highlight) or open a single incident. The user can then click on the “Action” pulldown and select either the “Run Rapid Report” or “Record Detail Report”. Both options allow the user to save the report in common software formats (Excel, MS Word, CSV, HTML, PDF, etc.)



- Run Rapid Report: The rapid report allows users to pull out data elements needed to complete the STD. 99 for CHP or the STD. 152 for DGS. Cal-CSIRS launches a window which allows the user to choose either template. The following screenshot is a sample of the output for the STD. 152.



- Record Detail Report: The record detail report allows the users to have a hard copy of the incident details, for archive (paper) files and reporting purposes.

6.3 Group Incident Report Procedures

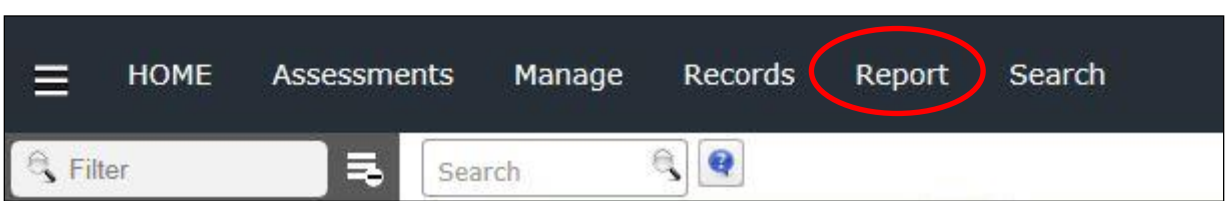
With the “Incident Navigator” open, the user can select the export button: 

Cal-CSIRS will then export the summary group data to an external file. Although only the Excel format is shown below, the user can export the report to other, common software formats (Excel, MS Word, CSV, HTML, PDF, etc.)

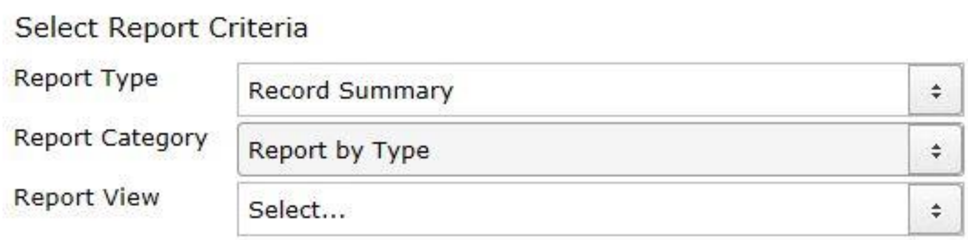
Once the incident data is exported, the user can edit, sort, and format the file for reporting requirements.

6.4 Advanced Report and Chart Procedures

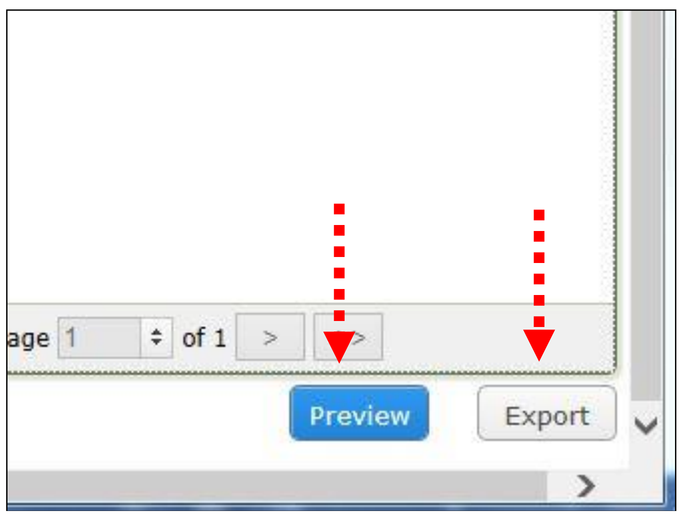
With the “Incident Navigator” open, the user can select the “Report” button, in the top, black bar.



Select a report type, category, view, and items to include in the report using the options below. Then click on Preview or Export to generate a report.



Cal-CSIRS will provide varoius report options. Select "Preview" (lower right corner) and change the various options to obtain the desired output. Select "Export" when ready.

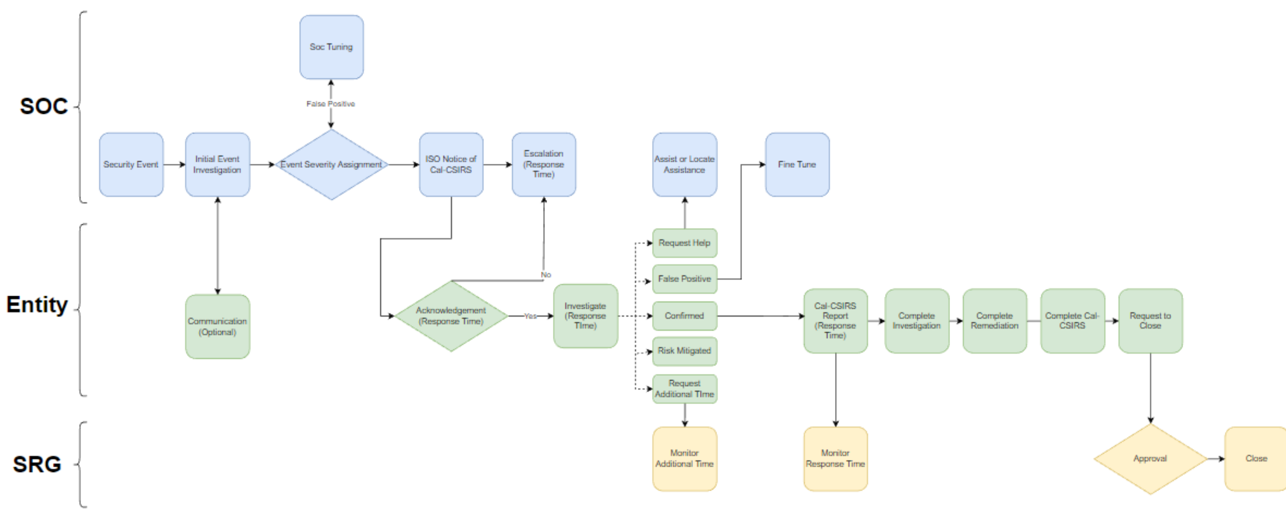


7.0 SOC SEN

7.0 SECURITY OPERATIONS CENTER SECURITY EVENT NOTIFICATION (SOC SEN)

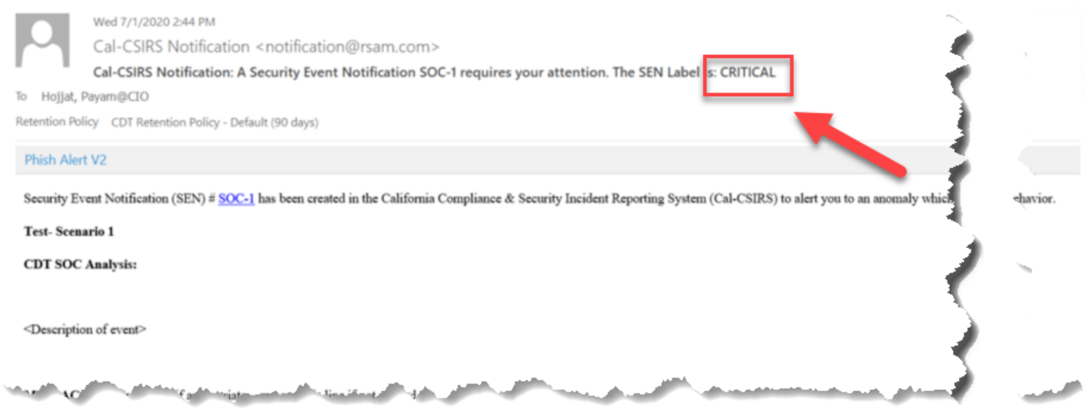
All traffic that is routed through CGEN is analyzed by the CDT SOC team. If anomalous behavior is detected, CDT's SOC will assess the events triggered from their monitoring tools, write a quick summary of the event, assign a criticality rating and send a notification to the affected parties about the activity, initiating a SOC SEN.

The SOC SEN is a workflow process integrated into RSAM, which enables fluid communication between the entity and CDT during initial findings of anomalous behavior. A separate SOC Navigator module will house all SOC notifications and tickets created by the CDT SOC team for any particular entity. When a SOC SEN is initiated, the CDT SOC team will create a SOC ticket for the affected party and incident, and will notify the ISO and Security team of the department via email. The initial email will request the entity to address the anomalous behavior and to run through the SOC SEN process of Acknowledgement, Identification, Reporting, and then any further Mitigating strategies needed as documented in the entities Incident Response plan. The following diagram outlines the current SOC SEN workflow and the responsibilities of each stakeholder.



7.1 SOC SEN Process Workflow

All SOC SENs will be labeled with a criticality level. The entity is to respond back to CDT with their decisions and/or findings within their appropriate reporting timeframes listed in the initial SOC SEN acknowledgment email and then follow the workflow process as needed.

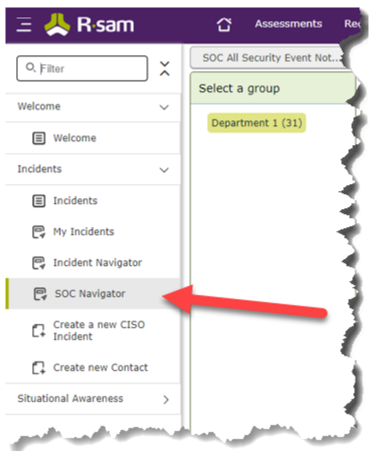

Wed 7/1/2020 2:44 PM
Cal-CSIRS Notification <notification@rsam.com>
Cal-CSIRS Notification: A Security Event Notification SOC-1 requires your attention. The SEN Label is: CRITICAL
To Hojjat, Payam@CIO
Retention Policy CDT Retention Policy - Default (90 days)
Phish Alert V2
Security Event Notification (SEN) # SOC-1 has been created in the California Compliance & Security Incident Reporting System (Cal-CSIRS) to alert you to an anomaly whic ehavior.
Test- Scenario 1
CDT SOC Analysis:
<Description of event>

Timeframe for Acknowledgement		Timeframe for Determination		Timeframe for Cal-CSIRS Reporting		Timeframe for Completing All
From the time an initial notification was sent an Entity Acknowledges Initial SEN Notification (Email or Cal-CSIRSSEN) Within...	Plus (+)	From the time an Entity Acknowledges Initial SEN Entity Makes Determination as Positive, False, Risk Accepted, Risk Mitigated, or Help or More Time needed Within...	Plus (+)	From the time, a Positive determination is made Entity Opens a Cal-CSIRS Incident Report Within...	Equals (=)	Entity Maximum Time Target
Critical (Red) 1 clock hour	Plus (+)	Critical (Red) 2 clock hours	Plus (+)	Critical (Red) 30 clock minutes	Equals (=)	Critical (Red) 3.5 clock hours
High (Orange) 2 Business hours	Plus (+)	High (Orange) 4 business hours	Plus (+)	High (Orange) 1 business hour	Equals (=)	High (Orange) 7 business hours
Medium (Yellow) 2 business hours	Plus (+)	Medium (Yellow) 4 Business hours	Plus (+)	Medium (Yellow) 2 Business hours	Equals (=)	Medium (Yellow) 8 business hours
Low (Blue) 8 business hours	Plus (+)	Low (Blue) 16 business hours	Plus (+)	Low (Blue) 2 business hours	Equals (=)	Low (Blue) 26 business hours

7.2 SOC SEN Acknowledgement

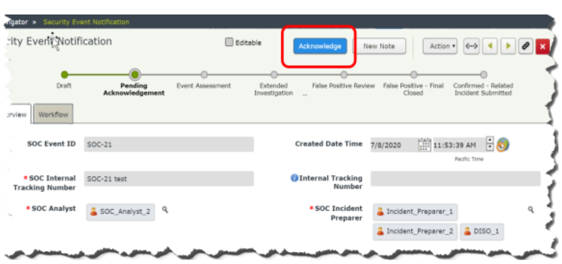
1. Once your department has received an acknowledgment letter from the CDT SOC team, stating that there is anomalous behavior stemming from your environment, the entity is required to address the issue immediately and acknowledge that they have received this notification. The entity will have to acknowledge the incident within the reporting timeframe of the criticality level before moving forward towards identification, reporting and further remediation.

2. Notifications can be acknowledged by logging into RSAM and navigating to the SOC Navigator Module.

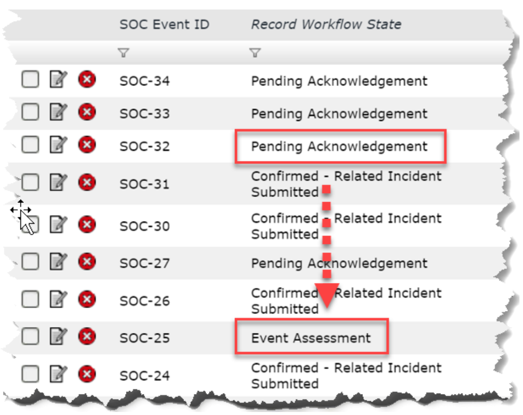


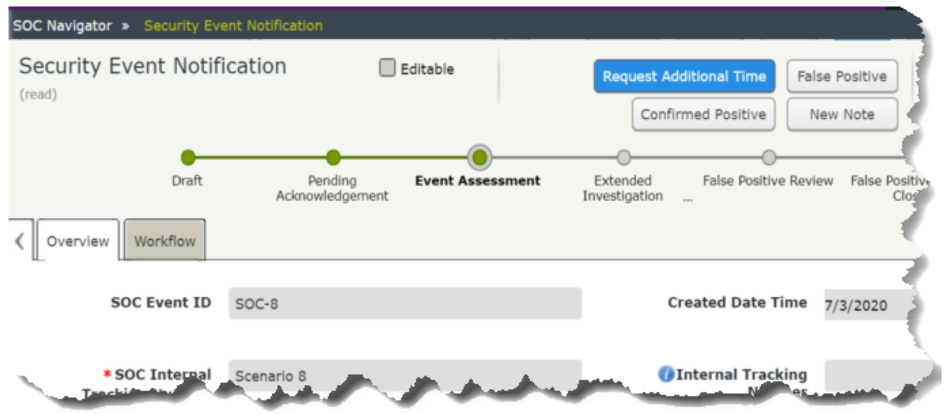
3. Once you identify the SOC Event ID correlated with you notification, you should see that the record state will be in a pending acknowledgment phase, which needs to be addressed.

4. After opening the associated SOC ticket record from your acknowledgement email. You will be able to acknowledge the activity by clicking the blue "Acknowledgement" button on the top right-hand corner. This will notify our CDT's SOC team that you are aware of the activity and will initiate an investigation and will report back with a decision within the reporting time frame.



5. Once acknowledged, the ticket will update its status to the "Event Assessment" phase, where then your department will be able to communicate back to the CDT SOC team to confirm a True Positive, False Positive, or Request Additional Time.

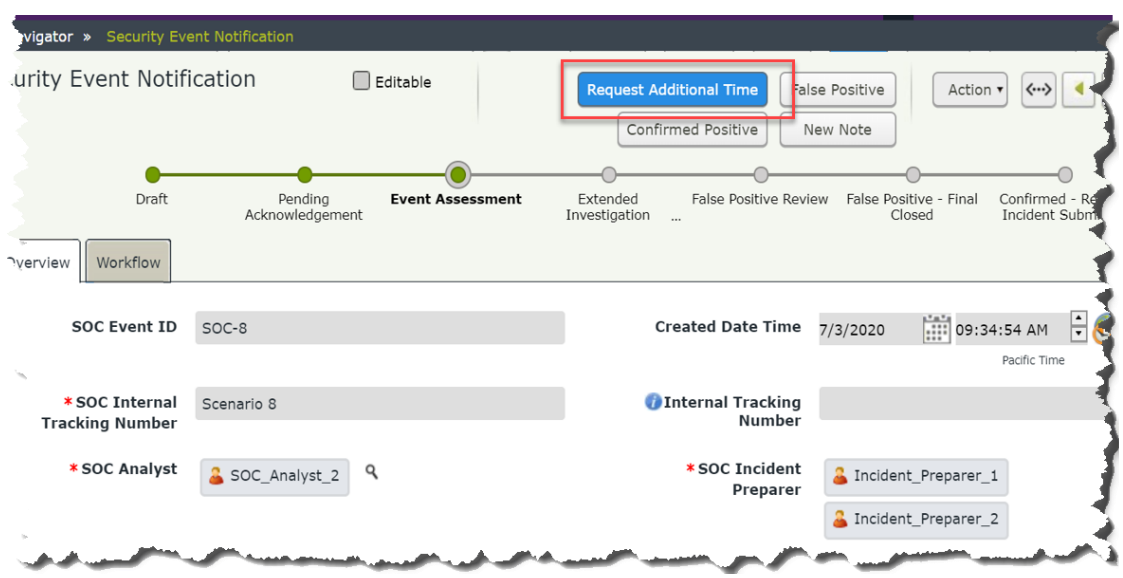




7.3 SOC SEN Request Additional Time

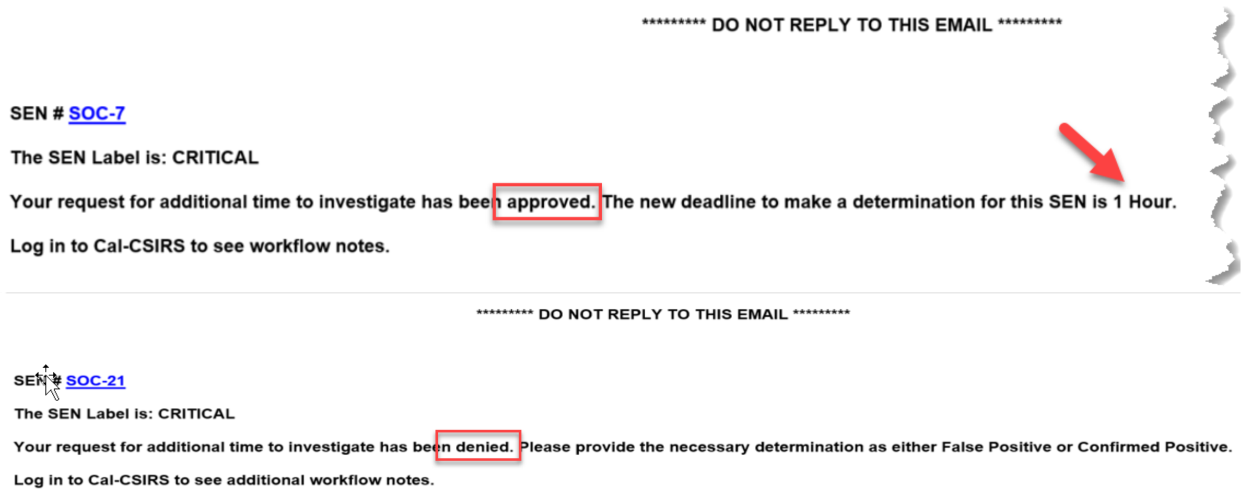
Based on the level of criticality of your SOC SEN notification, your department will only have a specified number of hours to determine if the incident was a True Positive, False Positive, or Risk Mitigated status. However, if you need additional time, beyond the standard reporting timeframe, entities have the option to request additional time. Once the entity requests additional time, the CDT SOC team will either approve and add additional time to their investigation or deny the request. Entities will only be allowed to request of an extension once per incident.

1. First you will need to identify and open the specific SOC ticket associated with your incident. Next, you can click the "Request Additional Time" button to initiate the request.



2. Once you request additional time, the CDT SOC team will either approve your request with a specific amount of additional time, or they will deny your request and your department will have to report the incident as a True Positive by creating a Cal-CSIRS ticket.

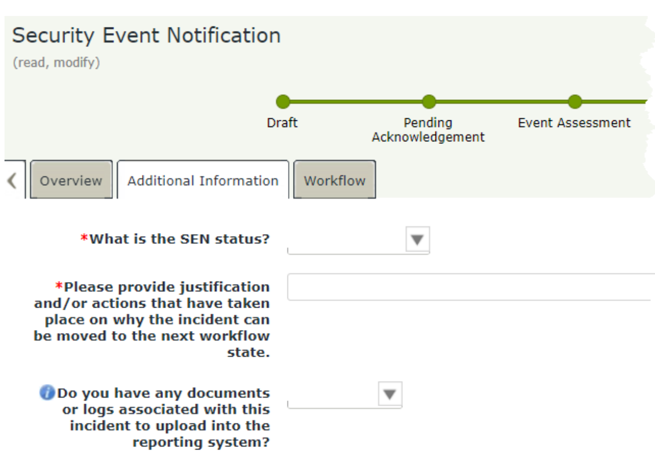
   If your department gets approved with additional time, and still goes beyond the additional time given, your department will then be required to create a Cal-CSIRS ticket and report the incident as a True Positive for the time being. (If at a later time it was determined as a False Positive, the Oversight Agencies can close the ticket out as a False Positive).



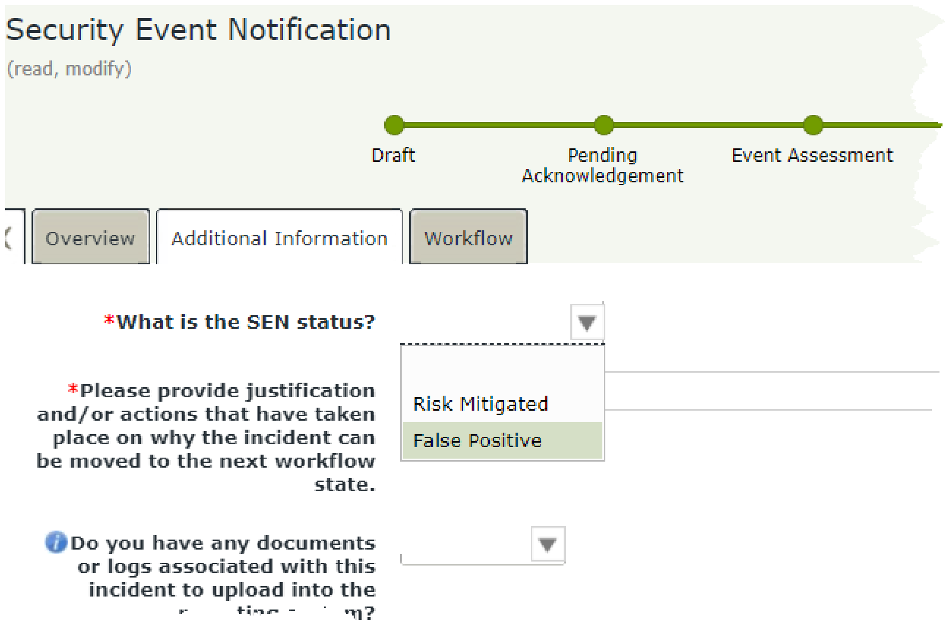
7.4 SOC SEN Reporting a False Positive

If you and your department were able to make a decision, within the specified reporting timeframe, that the notification from the CDT SOC team was a False Positive, you can report the SEN as a “False Positive”.

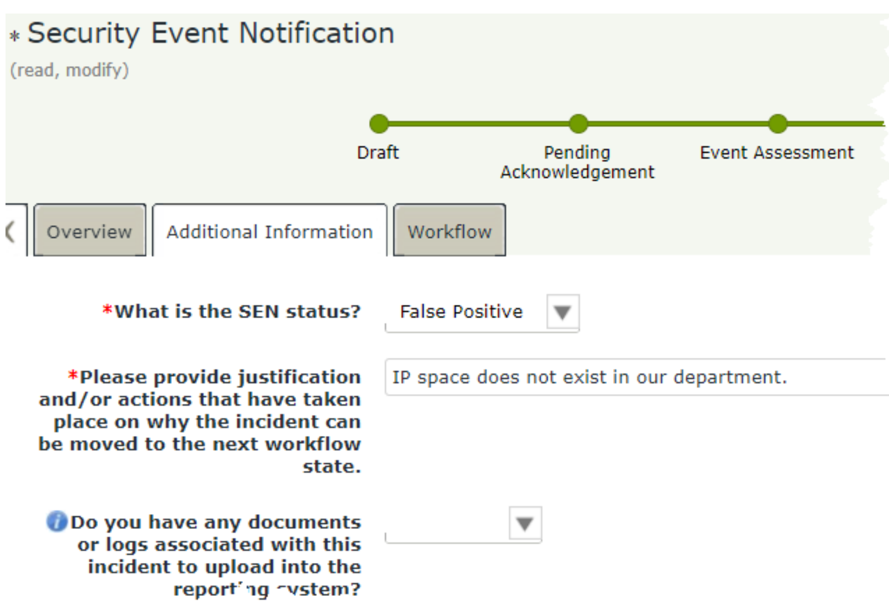
1. Open the SOC SEN and navigate to the “Additional Information” tab.



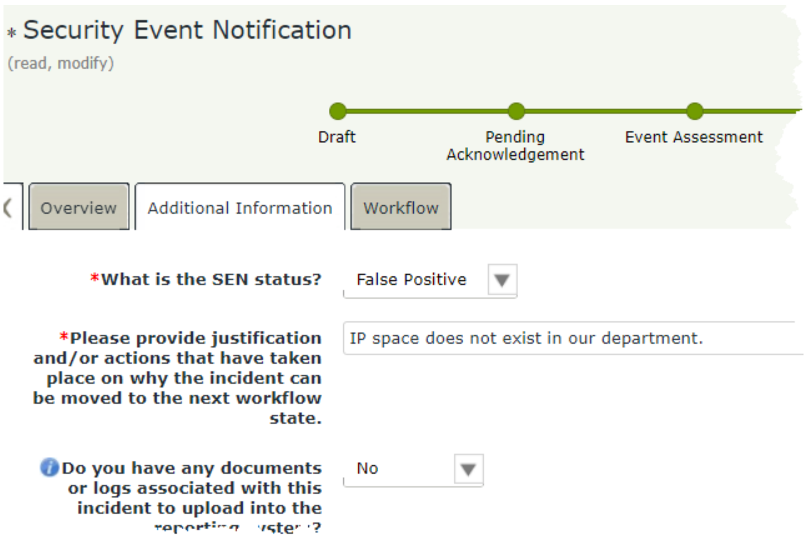
2. Fill out the additional fields of:
    a. What is the SEN status?



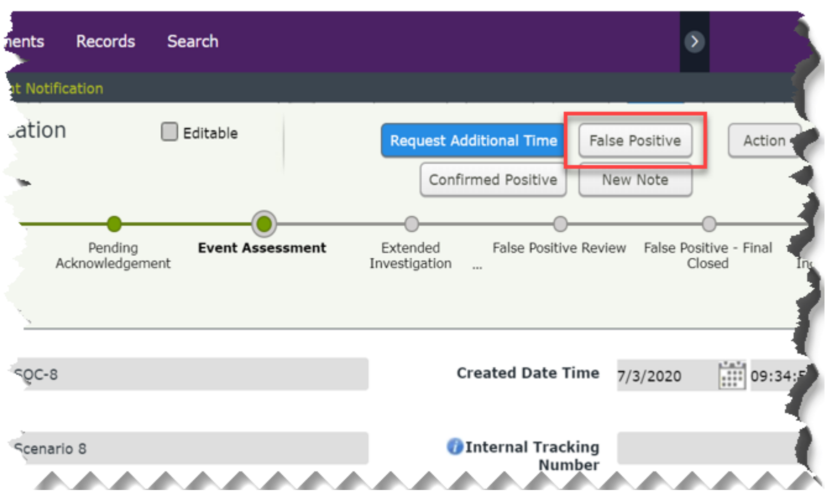
    b. Please provide justification and/or actions that have taken place on why the incident should be moved to the next workflow state. ***Please ensure that you provide as much detail as possible on action steps and investigation that took place to determine this SEN was a False Positive.***



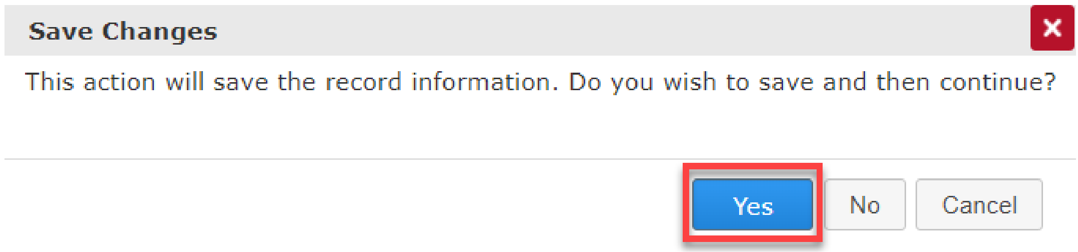
c. Do you have any documents or logs associated with this incident to upload into the reporting system? (Optional)



3. Next click on the False Positive button on the top right hand corner.

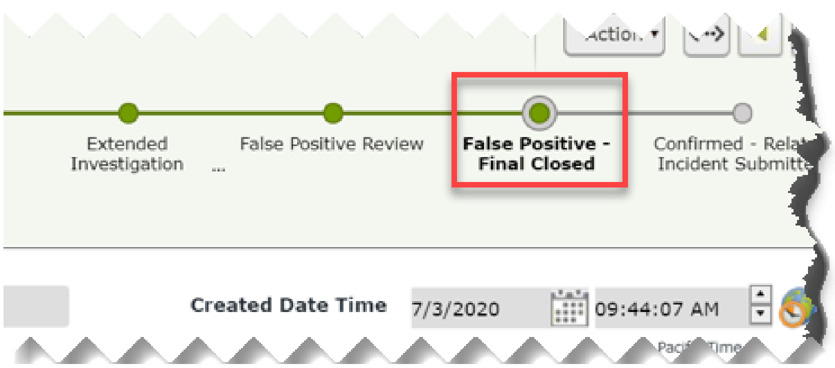


4. Once you have clicked the False Positive button, a pop window should appear requesting to save and confirm your action.



5. After you have successfully submitted your False Positive SEN, your department will shortly receive an email with a decision from the CDT SOC team on whether there is enough justification to close out the ticket and mark the event as a False Positive. If you receive an email stating that your "SEN has been closed.", the CDT SOC team has approved your False Positive decision and the SOC SEN notification has been resolved.

6. This will also move the status of the SEN to the "False Positive –Final Closed" status.

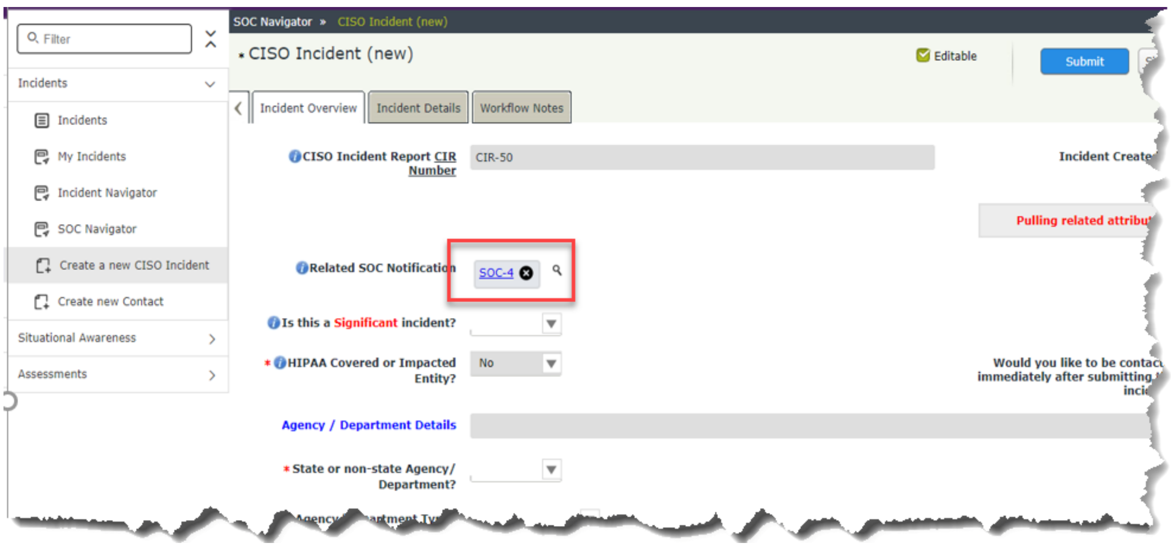


7. Otherwise, your department will receive an email notification stating that additional investigation is required. Your next options would either to be request additional time (if you have not already done so before), report a Risk Mitigated, or report a True Positive depending on the situation.

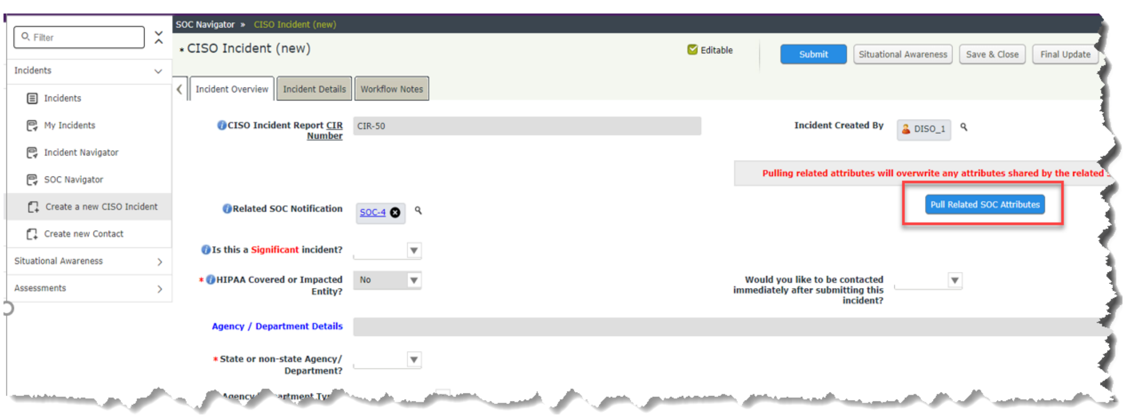
7.5 SOC SEN Reporting a True Positive

If your department has confirmed, or was requested, that a SOC SEN is to be a True Positive, your department will be required to create a Cal-CSIRS ticket. By creating a Cal-CISRS ticket, you will be able to associate the SOC SEN with the Cal-CSIRS ticket, confirming a True Positive, while closing the SOC SEN notification. In addition, when associating a SOC SEN, your department will be able to pull attributes and fields into the Cal-CSIRS ticket itself, streamlining the incident creation process.

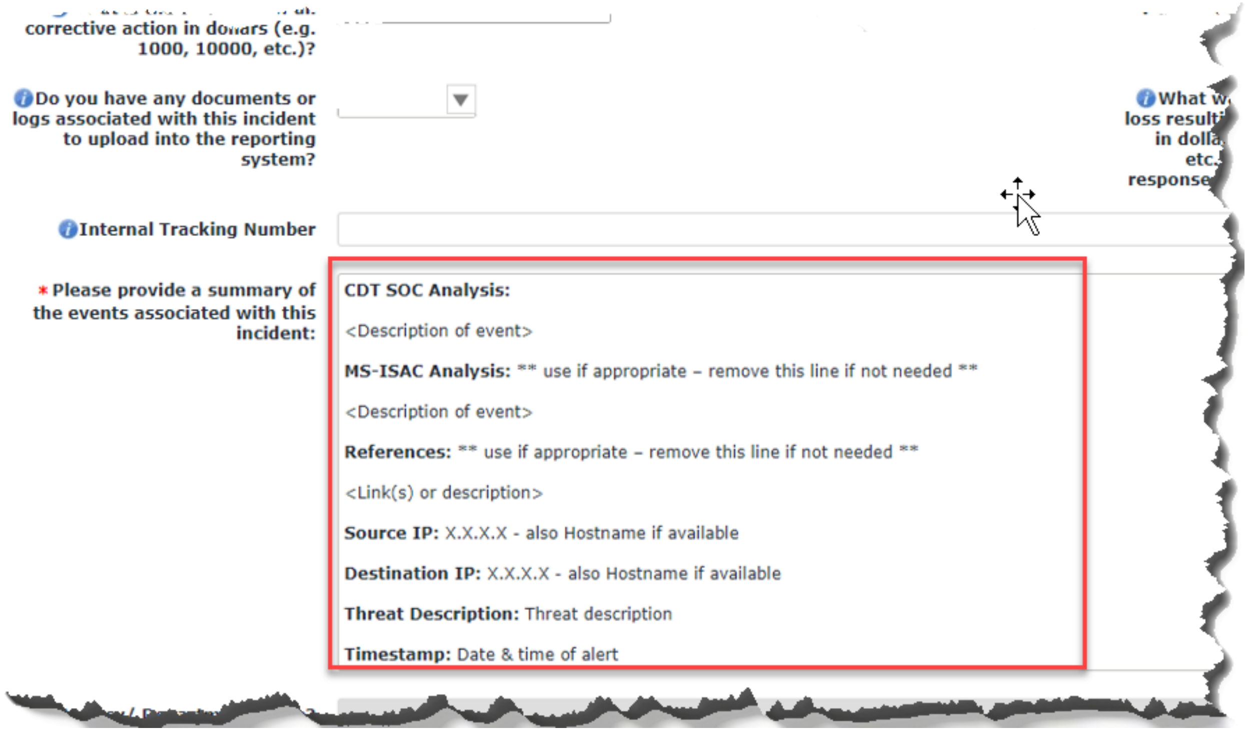
1. When reporting a True Positive, open and create a new Cal-CSIRS ticket as normal.
2. In the "Related SOC Notification" field, identify which SOC SEN ticket that you would like to confirm as a True Positive. After selecting and confirming the SOC related ID number, you should see the field populated.



3. Next, click on the "Pull Related SOC Attributes" button.

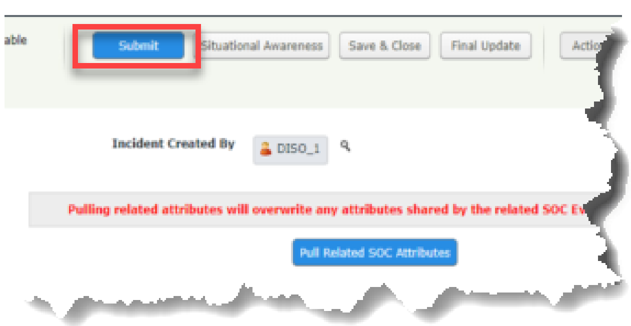


4. By clicking this button, attributes from the SOC ticket will populate the Cal-CSIRS ticket, which include the summary of events, department name, and other relevant fields associated with the incident..



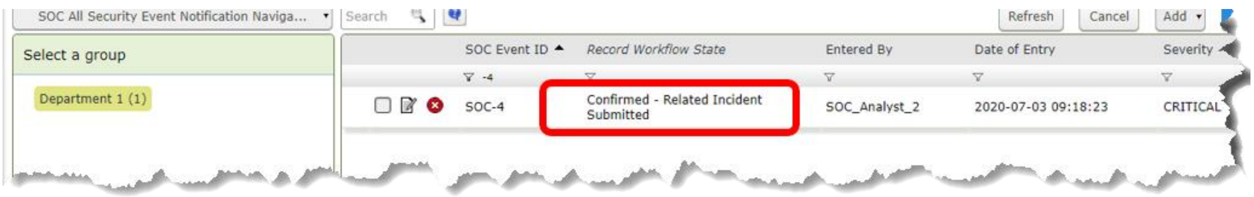
*** If you find any additional Indicator of Compromises or other relevant information during your identification phase, please update the summary field with your findings as well. Cal-CSIRS is a central repository in where all oversight agencies are able to view and gather details about the incident.*

5. After populating all the fields in the Cal-CSIRS ticket, click "Submit".

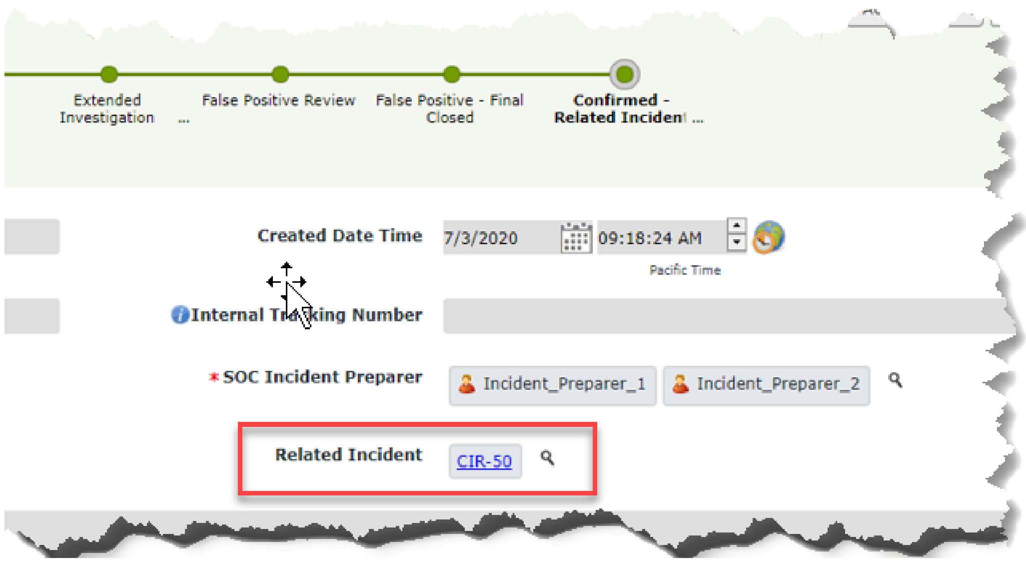


6. After reporting the Cal-CSIRS ticket, if you navigate back to the SOC Navigator and view your SOC ticket, you can see that the SOC ticket's status has been moved to "Confirmed – Related

Incident Submitted". No further actions will be needed from your department for the actual SOC ticket itself. However, your department will still be required to follow their dedicated Incident Response Plans and Playbooks until the confirmed breach has been fully resolved.



7. You can also open the SOC ticket itself and confirm the Cal-CSIRS associated to the SOC ticket. At this point, no further actions will be needed from your department for the actual SOC ticket itself. However, your department will still be required to follow their dedicated Incident Response Plans and Playbooks until the confirmed breach has been fully addressed.



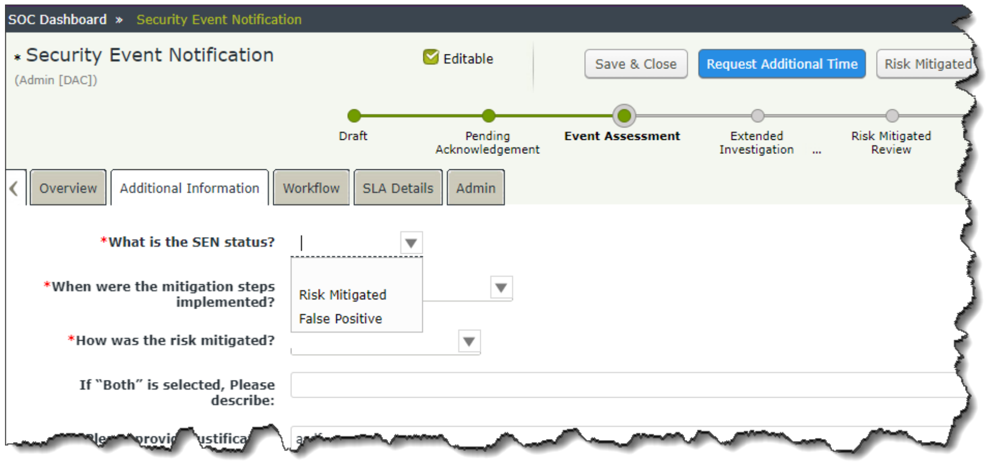
7.6 SOC SEN Reporting a Risk Mitigated

If your department has confirmed the presence of a threat/vulnerability, associated with the notification of a SOC SEN, and the reported activity has been mitigated before or after the SEN was received, your department has the option to close the SEN as being "Risk Mitigated". Having the SOC SEN as a Risk Mitigated confirms that the threat/vulnerability exists or existed; however, has not been exploited and that your department has actively taken mitigation steps to reduce or accept the risk. All actions taken to mitigate the risk must be documented in the SOC SEN.

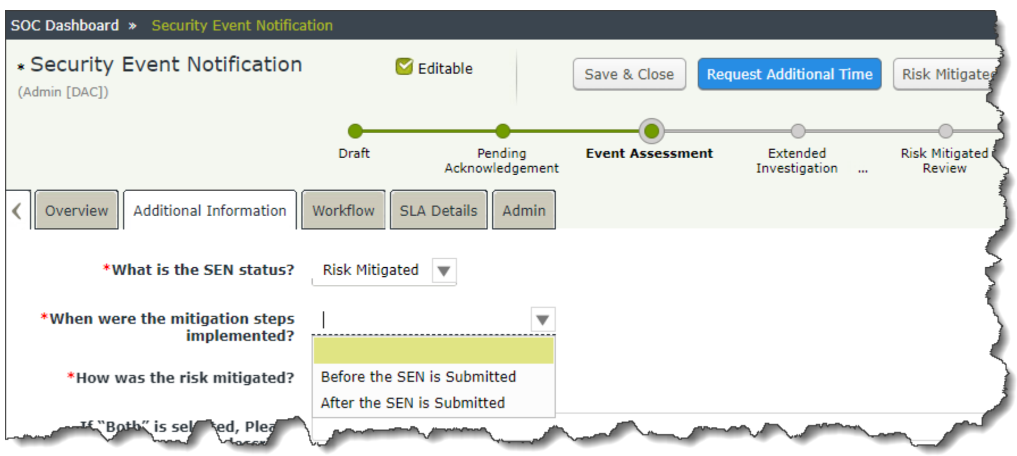
1. When confirming a Risk Mitigated SEN, in the Event Assessment workflow, navigate to the "Additional Information" tab.

2. Fill out the additional fields of:

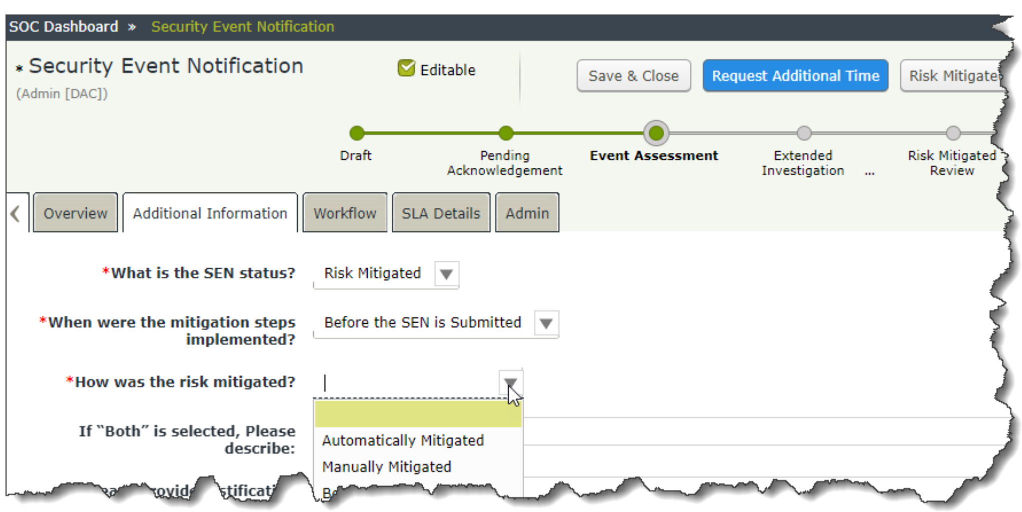
a. What is the SEN status?



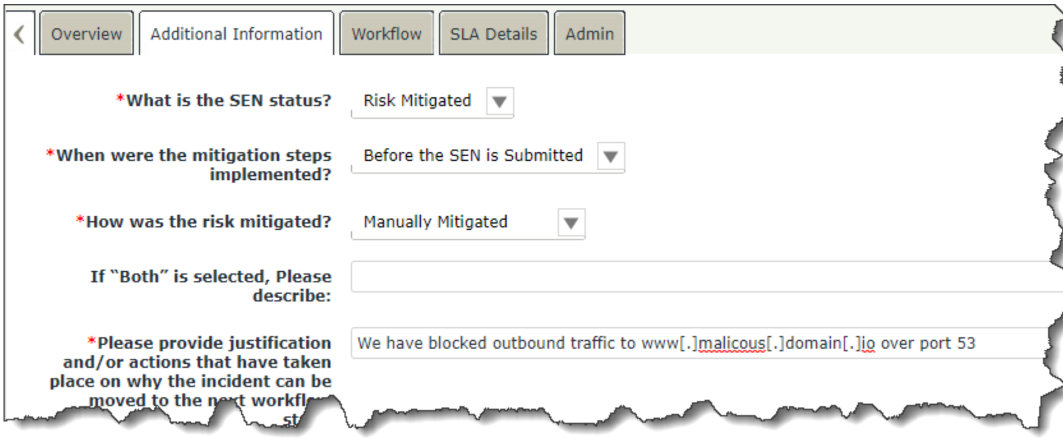
b. When were the mitigation steps implemented?



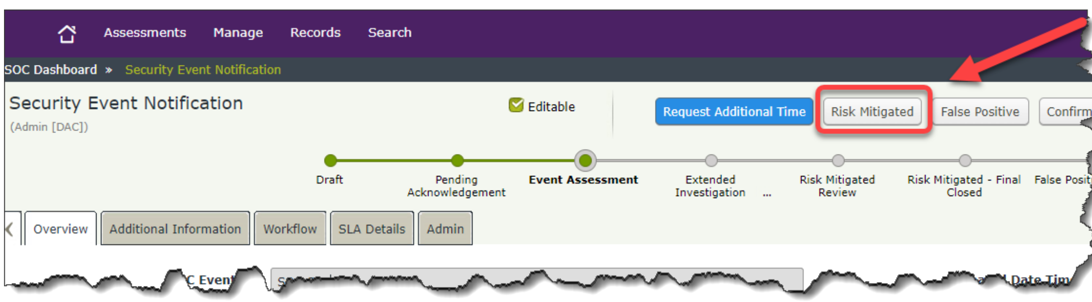
c. How was the risk mitigated?



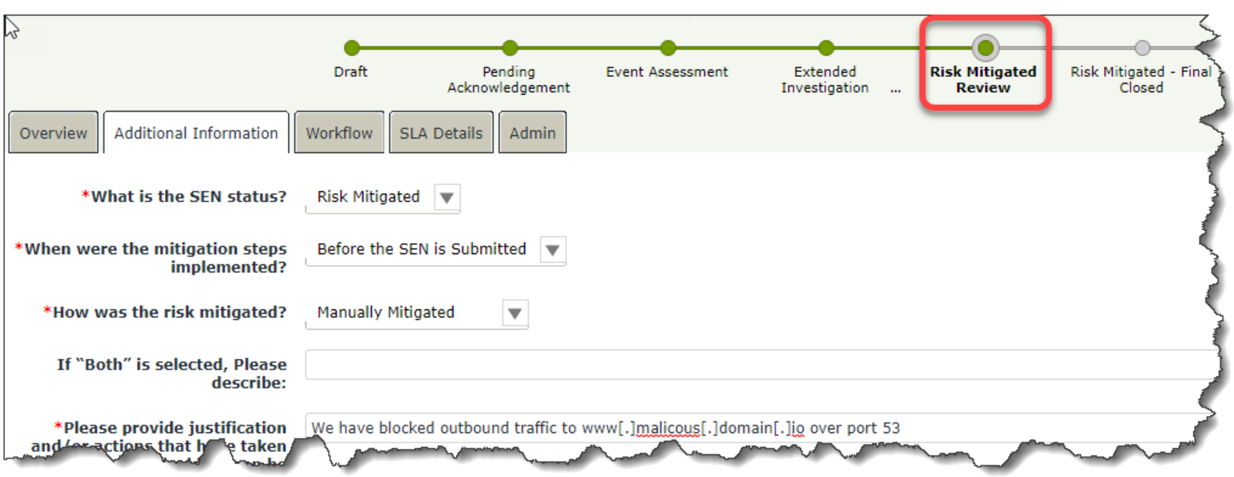
d. Please provide justification and/or actions that have taken place on why the incident should be moved to the next workflow state. ***Please ensure that you provide as much detail as possible on remediation and action steps taken to address the risk.***



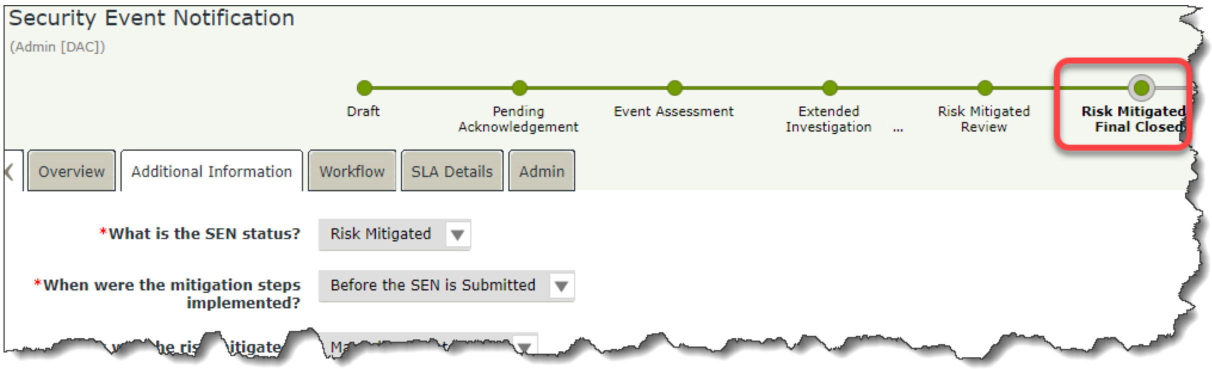
3. Once the additional fields are filled, click the "Risk Mitigated" button on the top right-hand corner.



4. After you have submitted your "Risk Mitigated" SEN, the CDT SOC team will review your request to close out the SEN.



5. If you receive an email stating that your “SEN has been closed.”, this means the CDT SOC team has approved your Risk Mitigated decision and that the SOC SEN notification has been resolved.
6. The workflow state of your SEN should now be moved to “Risk Mitigated - Final Closed)



APPENDIX

8.0 APPENDIX

8.1 Appendix – A Incident Questions

01 - DENIAL OF SERVICE ATTACK

Is this a Distributed Denial of Service (DDOS) attack?
What system is/was impacted?
If other, describe impacted system:
Name of the affected/targeted system?
Is the affected/targeted system mission critical and/or public facing?
If Other, please describe:

Make (DOS Attack):
Model (DOS Attack):
Type (DOS Attack):
Operating System (DOS Attack):
What type of central processing unit is/was involved (DOS Attack)?
What was the severity of the attack?
What resources are/were being impacted?
What known ports are/were involved?
What are/were the attack characteristics?
Who is your Internet Service Provider (ISP)?
If other, identify ISP:
What steps have been taken to contain or mitigate against the attack?
What is the attack method?
If other, identify attack method:

02 - MALWARE

What type of malware is involved?
If other, describe:
Did anyone pay the ransom?
Are there screenshots of the transaction (Ransomeware)?
Were there any files encrypted?
Was there permanent data loss or were there backup files available?
Are there “help_decrypt” or similar files available?
Is there an email(s) with the initial payload attached?
Is the name of the malware known?
What is the name of the malware?
Was the malware sent to anti-virus vendor for analysis?
What type of system was infected?
Other Infected Type

How was the malware introduced?
If other, describe:
What are the characteristics of the malware?
Describe Other Mawlare Characteristics
Was the network accessed by the malware?

Did the malware facilitate the release of information?
What anti-virus product was in use on the affected device or system?
If other, describe:
What was the anti-virus product version in use on the affected device or system?
Did the anti-virus product detect the malware?
Was the affected device or system scanned with another security scanning tool?
If YES, did any other security scanning tool detect the malware?
If YES, please explain:
What action was taken when malware was detected?
If other, describe action taken:
What steps have been taken to contain the incident?
Were other infected devices identified?
How was this determined?
What method(s) were used to identify and isolate other infected devices?
If other, please explain:

3 - INFORMATION ASSET (PROPERTY) LOSS OR THEFT

Do you have information about any other individual(s) associated with this incident, such as victims, witnesses, employees or suspects, who can provide additional information about this incident?
Associated Type:
Type of location where the incident occurred?
If other, describe:
Do you wish to generate the REPORT OF CRIME OR CRIMINALLY CAUSED PROPERTY DAMAGE ON STATE PROPERTY report (state form STD. 99) at this time?
Do you wish to generate the PROPERTY SURVEY REPORT (state form STD. 152) at this time?
Do you have any information asset (property) to report as lost, stolen, or damaged?
If YES, describe:
Make/Brand/ Model:
Serial number (if available):
State asset tag number (if available):
State owned/leased?
Privately owned?
Property damage?
If YES, estimated damage value?
Property loss?
If YES, estimated value of property?
If state owned property was lost, stolen, or damaged, where was property located when incident occurred?
If other, describe location:
If you are reporting lost or stolen state property that is a piece of information technology equipment, did it contain state owned or personal identifying information?

a. Was the information contained on the piece of equipment encrypted?
b. Was the piece of information technology equipment password protected?
c. Was the piece of information technology equipment capable of being remotely wiped?
d. If YES, was it remotely wiped?

4 - INFORMATION DISCLOSURE

e. What classification of information was disclosed?
f. What type of media/format was involved?
g. What type of personally identifiable information was involved?
If other, describe:
h. What best describes how information disclosure occurred?
If other, describe:

5 - MISUSE

How is the alleged misuse best described? (Check all that apply)
If other, describe:
Do you suspect this incident involves fraud, embezzlement, or other criminal activities?
Do you have an identified individual responsible for the alleged misuse?
What level of access rights does the individual responsible for the alleged misuse have? (check all that apply)
Who owns the system the misuse is associated with?
Does the involved agency/department have software that monitors internet usage for all users?
Please Describe:
Is the internet history available for the alleged misuse?
What type of system was accessed? (Check all that apply)
Was confidential, personal or sensitive information associated with the misuse?

6 - OUTAGE OR DISRUPTION

If other, describe:
If mission critical system, what is/was the business function?
Did the outage trigger emergency response or technology recovery plan activation?
What other entities or constituencies were/are impacted by the outage or disruption? (check all that apply)
Describe other impacted entities
Is the outage or disruption still in progress?
If YES, what is the estimated timeframe for resolution?
If NO, what was the total duration of the outage or disruption?

7 - SOCIAL ENGINEERING / PHISHING

What is the source of the phishing attack? (check all that apply)
If Other, please describe:
What information was sought in the phishing attack? (check all that apply)
If Other, please describer:
Was the attack successful? (information provided by victim)
Was the phishing attack directed at an individual? (spear phishing)
Is the original phishing email(s) with header(s) & footer(s) available?
Do you have a screenshot(s) of the phishing email?
If YES attach Phishing email screenshot:
How many users received the phishing email or telephone call?
How many users actually provided personal identifying information as a result of this attack?
When was the last time your agency issued an alert or warning about email phishing attacks?

8 - UNAUTHORIZED ACCESS

What best describes the unauthorized access?
If other, describe:
Where did the unauthorized user gain access?
What system(s) was accessed? (Check all that apply)
If other, describe:
Make (Unauthorized Access):
Model (Unauthorized Access):
Type (Unauthorized Access):
Operating System (Unauthorized Access):
What type of central processing unit is/was involved (Unauthorized Access)?
How was unauthorized access detected? (check all that apply)
Did you scan for possible malware?
What were the results?
Do you know the source of the unauthorized access?
What is the source?
Is the individual involved in the unauthorized access subject to a clearly defined user access policy?
Does the agency/department have a current user access login in banner?
Was information acquired through this unauthorized access?

9 - UNAUTHORIZED DATA DESTRUCTION

When the data was destroyed, what type of media did it reside on?
If Other, please describe:
What type of data was destroyed?
If Other, please describe:
Did the destruction of data occur as a result of an intrusion from an external source?

10 – FRAUDLULENT ACTIVITY

Was the fraudulent activity successful?
Has this been a recurring issue?
Has the root cause been determined?
Is there an ongoing active law enforcement investigation?
Specify lead Law Enforcement entity with case number.
Through what mechanism or IT system was the fraudulent activity conducted through?
How did the fraudulent activity happen? Please provide as much detail as possible?
Was there an Identity Verification and Management control Implemented?
What kind of Identity Management has been implemented?
Why has there been no Identity Management implemented?
Is the lack of Identity Management on your POAM?
Did the activity result in a loss to the beneficiary or the State?
What program was impacted?
Was there any money embezzled?
How much was embezzled?
What type of fund was the money taken from?
Was this a cyber related incident?
Was there a compromised account or device?
Is there information that suggests that the threat-actor was attempting to gain unauthorized access to: (check all that apply)

Is there information that suggests that the threat-actor was attempting to create new User Accounts.
Was there any sensitive information involved, stolen, or used?
What type of PII was disclosed?
Has the root cause been fully addressed?
Explain why not and your plan of actions and milestones to fully address?

8.2 Appendix – B Frequently Asked Questions about Cal-CSIRS

1. **What if I am in multiple roles for multiple entities?**
   Response: You will be issued a single user-id and password that can connect to each of your entities.

2. **What if my entity needs more than one alternate reporting designee who can report incidents?**
   Response: Unfortunately we are unable to accommodate the request for additional user accounts at this time. We are able to provide each state entity with a total of three Cal-CSIRS user accounts. One account will be assigned to the designated Chief Information Officer (CIO) and one account will be assigned to the designated Information Security Officer (ISO). The entity may choose one alternate designee for the third account. To ensure that the CISO office is providing access to accommodate the assigned reporting structure, it is crucial that we provide the primary CIO and the primary ISO access into the Cal-CSIRS system.

   CIOs and Information Security Officers (ISOs) are designated by their Directorate (entity head) in accordance with legal and policy requirements (Government Code 11546 and SAM 5330), and are responsible for keeping their Directorate informed of risk and incident related matters. Therefore we are ensuring that all the primary CIO and ISO designees have access to the Cal-CSIRS reporting system and one alternate of the entity's choosing are able to access information reported on behalf of their entity and the management report capabilities so that these individuals will be able to keep their Directorate fully informed.

   We understand the need for additional user accounts and are looking into an enterprise licensing approach that may accommodate additional user accounts in the future. Please feel free to contact our office if you have further questions.

3. **Will our AIO and AISO have access to all of the Departments included within their Agency?**
   Response: Yes, the security model is designed to segregate the agencies and department views.

4. **How do I change the selected alternate reporting designee?**
   Response: If the alternate reporting designee information needs to be changed, notification must be made by the CIO or ISO to CISO at security@state.ca.gov. Our Office will provide you with the Cal-CSIRS reporting designation form and instructions.

   Note: The Cal-CSIRS reporting designation form is separate from the annual Agency Designation Letter (SIMM 5330-A) and facilitates access and authentication preferences for Cal-CSIRS. If you have a change in your CIO or ISO designation you will still use the SIMM 5330-A.

5. **How does my new designee obtain the Cal-CSIRS User Manual?**
   Response: When a completed Cal-CSIRS reporting designation form is submitted to our Office, a Cal-CSIR User Manual will be sent to the new reporting designee.

6. **Is there a new incident number scheme for Cal-CSIRS?**
   Response: Yes, Cal-CSIRS has a new number scheme.

7. **Will previous SIMM 5340-B incidents be uploaded into Cal-CSIR?**
   Response: No. It is not feasible to import CHP and CISO data from existing and disparate reporting systems to the new system. We will implement a clean cut-over from the old reporting process to the new Cal-CSIRS reporting process.

8. **If California Highway Patrol (CHP) Computer Crimes Investigations Unit (CCIU) decides to investigate will they or the Emergency Notification and Tactical Alert Center (ENTAC) give me a separate number for the same incident?**
   Response: CHP will use the Cal-CSIRS number; thus, CHP and CISO will now use the same number.

9. **Will an entity be able to print an individual incident report?**
   Response: Yes. Initially the individual report will print all possible questions and any answers to those questions.

10. **Will an entity be required to print and route a hard-copy of the report for signatures?**
    Response: No, with the implementation of Cal-CSIRS, routing a hard-copy for signatures will no longer be required. State entities must continue to inform their Privacy Officer, CIO and department director of incidents in accordance with state policy on incident handling and coordination (SAM 5340.3 and SAM 5340.4) instructions and procedures (SIMM 5340-A) as well as in accordance with their internal organizational processes and procedures. Further, the system will allow entities to create reports of open and closed incidents to facilitate Security Governance and Executive Management briefings.

11. **Will Cal-CSIRS generate either the Std 152 or Std 99 form?**
    Response: Cal-CSIRs will allow you to print the data input into Cal-CSIRS to assist with preparing those reports. However, because those reports require much more information than Cal-CSIRS requires, you will still need to complete the Department of General Services Std 152 and California Highway Patrol Std 99 forms if applicable to the incidents you report through Cal-CSIRS, and send them to DGS and CHP.

12. **Will Two Factor Authentication (2FA) be required to access Cal-CSIRS?**
    Response: Yes. State entities will provide Cal-CSIRS user contact information for receiving the randomly generated code to our Office through the Cal-CSIRS reporting designation process. At login, the system will generate a one-time code to enter along with user id and password.

13. **Will 2FA be required each time a user logs into Cal-CSIRS?**
    Response: No. 2FA will only be required once during the day if you are logging in/out/in on the same device.

14. **Since each profile is tied to their role (AIO, ISO for example) and the departments and/or agencies that they will have privileges for, why can't the profile be further customized and automatically answer some questions, which could be overridden if necessary. For example, if I am a department that does not have HIPAA requirements, why can't that question be automatically be set to "no" for my profile?**
    Response: This is not currently part of the profile but we understand the need to continue to simplify wherever possible. A Cal-CSIRS user group will be established to facilitate identification, prioritization and general governance of future changes and enhancements.

15. What will be the retention policy for incidents in Cal-CSIRS?
Response: It will be in accordance with our Department's current retention policy for these records, which is currently 5 years from the date an incident is closed.

16. Is the data in Cal-CSIRS subject to Public Records Act (PRA) requests, or exempt from PRA pursuant to Government Code Section 6254.19
Response: Yes, these records are subject to PRA requests. However, some data within Cal-CSIRS may be considered confidential and exempt from disclosure. For example, records for which the disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency (Government Code Section 6254.19). The Department's process is to review all requested records and redact when necessary the protected or otherwise exempt portions of the record before its release.

17. What is the "Situational Awareness" button?
Response: The situational awareness button allows a reporter to share information about anomalous or suspicious activity they've observed that has not risen to a reportable incident for their entity. As an example, a large department may wish to share that it is seeing an unusually high volume of traffic from a specific IP or IP range. The situation may not have resulted in an outage or disruption but could impact others and would be worth sharing. To create a Situational Awareness Report use the "Situational Awareness" button instead of the "Submit" button.

18. Who can see and who is notified when the Situational Awareness reports made through Cal-CSIRS?
Response: All Cal-CSIRS users may see a Situational Awareness report. The SAR allows the community to share information about suspicious activity trends and anomalies (for example an uptick in probe and scan activity) that may not constitute a reportable incident.

19. Who can see and is notified when a department submits an incident report?
Response: Authorized representatives from CHP's Emergency Notification and Tactical Alert Center (ENTAC) and Computer Crime Investigations Unit (CCIU), authorized representatives from the California State Threat Assessment Center system, and authorized representatives from the California Information Security Office (CISO), and authorized users in the reporting entity and its Cabinet-level Agency may see reports submitted by a department. Cabinet-level agencies have visibility of all entities reporting up to them. An email alert is sent only to authorized representatives from CHP's Emergency Notification and Tactical Alert Center (ENTAC) and Computer Crime Investigations Unit (CCIU), authorized representatives from the California State Threat Assessment System, and authorized representatives from the California Information Security Office (CISO) when an incident is reported. Once reviewed by CISO an acknowledgement is sent to the reporting entity.

20. How will communications occur between CISO and reporting entities?
Response: Cal-CSIRS is an incident reporting system not an incident management system. Conversations needed to manage incident response will still need to occur by telephone, but these can be documented and preserved as part of the report record in the workflow notes, and notes/comments fields.

21. How will communications occur between CCIU and reporting entities?
Response: Cal-CSIRS is an incident reporting system not an incident management system. Conversations needed to manage incident response will still need to occur by telephone, but these can be documented and preserved as part of the report record in the workflow notes, and notes/comments fields.

22. I am an authorized reporting designee for my Agency, may I submit an incident on behalf of a department that reports up to our Agency?
Response: Yes. Please contact CISO if you need assistance with doing so.

23. I am an authorized reporting designee for my Department, may I submit an incident on behalf of another state department that we have an information exchange or system interconnection with business relationship with?
Response: No, the other department's authorized reporting designee will need to report the incident.

24. How is an incident closed?
Response: CISO will review reported incidents for completeness and will work with reporting entities to determine when they may be closed. Authorized reporters/preparers may update information in the system as it becomes available using the Save and Close button. Once the entity believes all required information has been entered they may select the Final Update button and this will send a notice to CISO

25. May we add additional information after an incident is closed?
Response: No. If needed, you may contact the CISO to make the needed comment/note.

26. How do we report an incident if Cal-CSIRS is offline?
Response: You will contact the California Information Security Office (CISO) during business hours to report the system is offline, and you or a CISO representative will enter your report once the system is back online. If after regular business hours you require immediate law enforcement assistance you will contact the CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. Note: ENTAC is only to be contacted when immediate law enforcement assistance is needed after regular business hours.

27. What is the Risk Assessment tab?
Response: Cal-CSIRS is designed to be a fully integrated governance, risk and compliance reporting system. The Risk Assessment module is for future use and has not yet been enabled.