Crime Insight Release Notes v4.0.1

Crime Insight version 4.0.1 was released on May 26, 2025.

What's New?

This version of Crime Insight contains seven significant updates:

a) Some NIBRS validation rules have been tweaked
b) The Users page has been re-implemented and the user interface updated
c) The Agency Dashboard has been updated and can now be enabled in any state
d) The Notices functionality has been updated and can now be enabled in any state
e) The Audit tool is released and can now be enabled in any state
f) Agencies in Tennessee can now submit NIBRS submissions automatically via web service
g) The Victim Cube in CO has been extended for improved performance of Domestic Violence reports

Note that although the Agency Dashboard, Notices and Audit can be enabled in any state, there is an extra charge for this functionality. Each of these is described in more detail below.

Validation Rules

As described below, RMS systems in Tennessee can now submit data automatically to Crime Insight for real-time validation and submission. As part of doing this project, there was a thorough review of many of the NIBRS validation rules implemented in Crime Insight and a few small changes were required.

The following changes affect all states:

- Error 084 is no longer reported when an incident includes offense 250 (Counterfeiting). Previously only offense 280 (Stolen Property Offenses) allowed property to be recovered that wasn't originally stolen.
- Error 705 is no longer reported by Crime Insight. Arrests in the future (based on the current date) result in error 765 being reported.

The following change affects all states that accept flat file submissions:

- Flat file submissions with zero reports with bad dates now result in the entire file being marked as "Failed". Previously, the system was trying to store those bad dates in the database resulting in other issues.

The following change affects all states that accept XML submissions:

- Crime Insight now rejects files where a <person> element is used for multiple offenders, victims or arrestees. Note that it is expected/encouraged that if a single person plays multiple roles (e.g. offender and arrestee) that they be represented by a single <person> tag, but one person cannot be multiple offenders (for example).

The following changes affect TN only:

- Error 751 is now reported when multiple Group B records with the same sequence number are provided.
- The <ItemQuantity> tag is ignored for any property that isn't a vehicle involved in an offense 240 (Motor Vehicle Theft). Ideally, this situation would result in a warning, and the warning will be provided for any agency validating records using the web service.

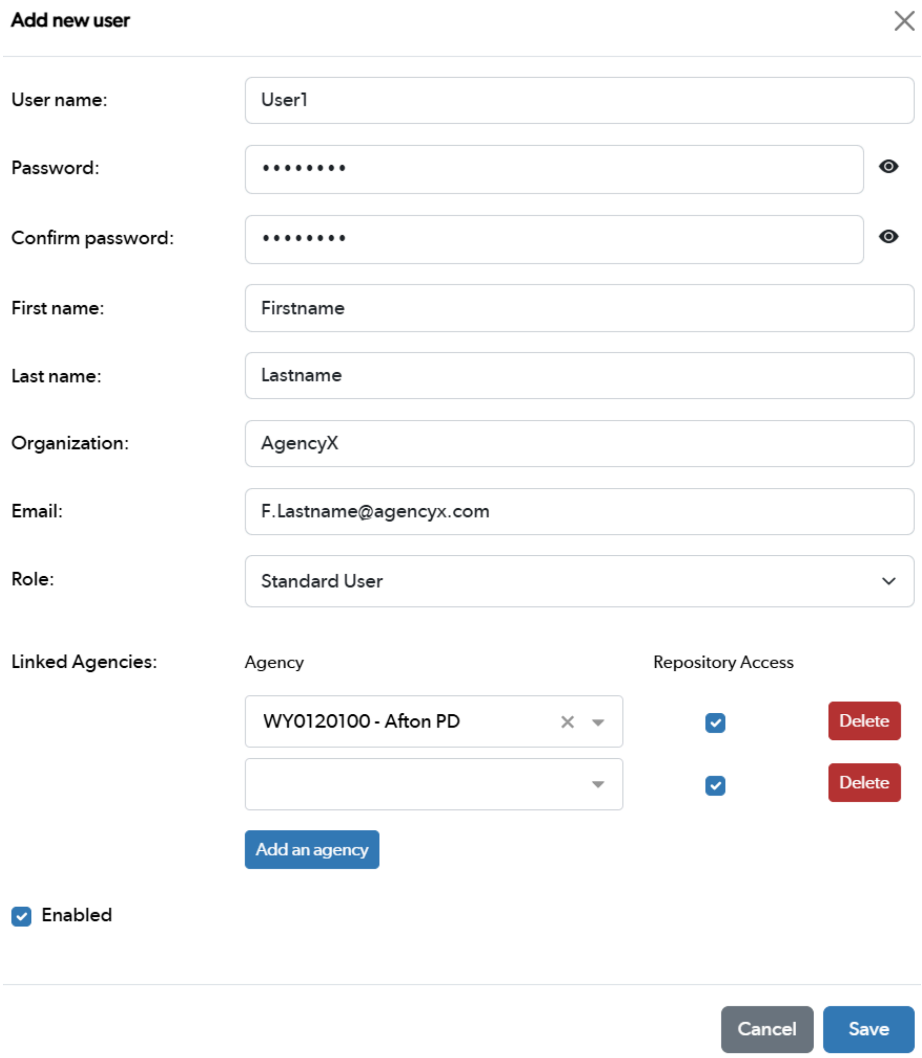
Users

The Users page has been updated to the new look-and-feel that will eventually be the standard across all pages. It uses the new Filter button, allowing administrators to filter the table by any column, making it easier to find users with specific criteria.

The dialog box for adding/editing user details has been updated as well. There are two significant changes:

- When adding agencies to users, this is now done using a drop-down list, making it easier to select the right agency for each user.
- The "Allow Upload" checkbox, which was always confusing, has been relabelled to "Repository Access". This is a more meaningful label for the checkbox's function:
    - On the LEA Reporting site, users will be able to create reports using any agency attached to their user account. (Note that in some states, this is irrelevant, as all agencies can see each others' data anyway.)
    - In the Repository, users can only see data for agencies where the checkbox is checked.

The following screenshot shows an example of the New User dialog box:



Agency Dashboard

The Agency Dashboard is designed to be the landing page for agency users connecting to Crime Insight. It gives an overview of the agency's status, notices (see below), upload history and statistics, and other useful information for the agency. The Agency Dashboard is laid out in a series of blocks. Users see only those blocks for which they have the appropriate permission enabled.

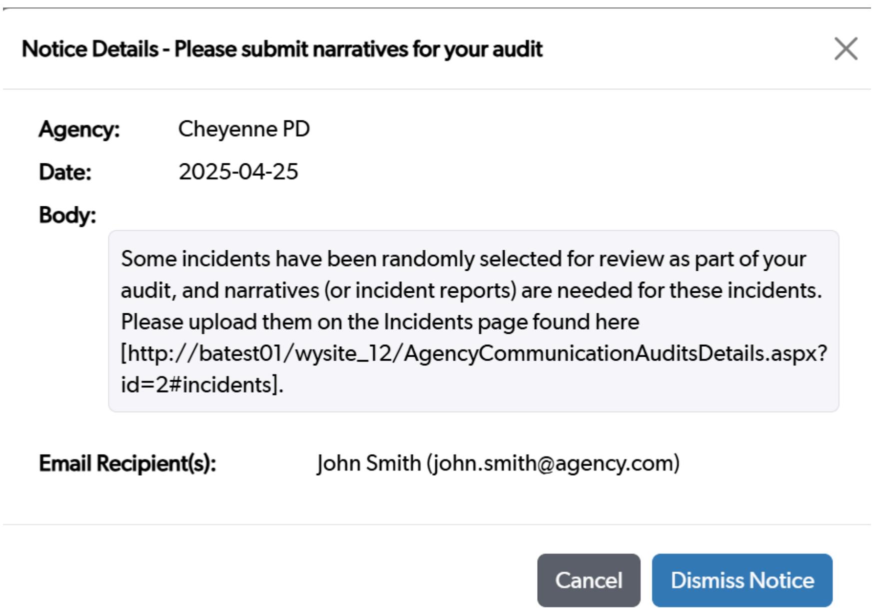
At the top of the Agency Dashboard, there is an agency selector. Users with access to more than one agency can use this selector to pick the agency that they want to view.

Block 1: Notices

This section only appears when the site administrator has sent a notice to the agency being shown. The headline for each notice is shown, along with the date when it was sent. There is a button to view the details of the notice. When viewing the notice details, the user can dismiss the notice, meaning that it is no longer shown on the Agency Dashboard (but is still available on the Notices page).

This section is shown only if the user has access to read notices directed to the agency.

The following screenshot shows a sample of the Notices section, and the details of a Notice:



Block 2: Data Collections

This section shows summary information for one data collection. There is a selector at the top to pick the data collection to be shown. This list contains all data collections the user has access to and that the agency is currently marked as submitting. The Agency Dashboard supports the following data collections:

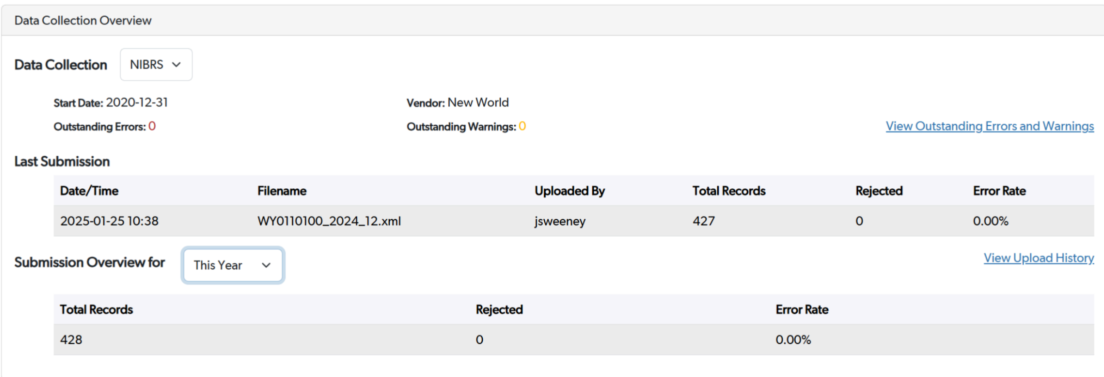
- NIBRS
- Use of Force
- Contacts (CO Only)
- Community Policing (CO Only)

Note that although Police Employee counts are also a data collection, this information is presented lower on the page, along with population information.

For each data collection, the box shows the following information:

- Agency start date
- Agency vendor
- Number of outstanding errors and warnings
- Details of last submission
- Statistical overview of number of submissions and rejections, aggregated for the current day, week, month or year.

The following screenshot shows an example of the information:



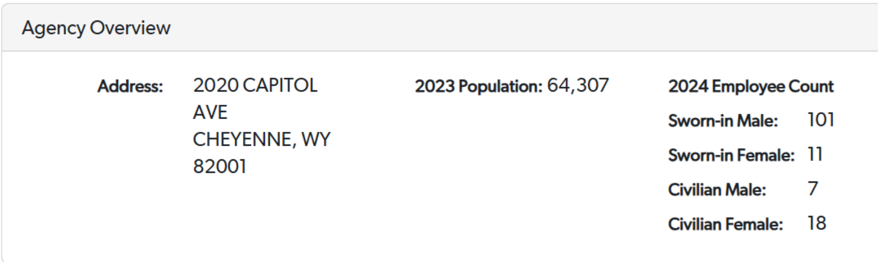
Block 3: Agency Overview

The Agency Overview section of the Agency Dashboard shows some general information about the agency. This includes:

- The agency's address
- The agency's most recent population (including the year for which it applies)
- The agency's most recent police employee counts (if the agency is participating in that data collection)

This section can be enabled or disabled by permissions.

The following screenshot shows an example of the information:

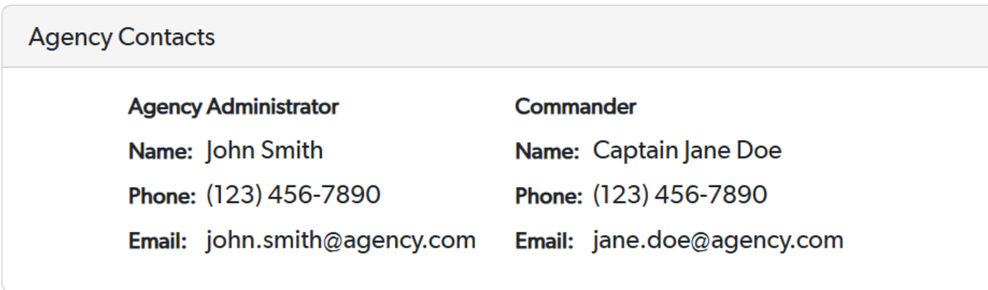


Block 4: Agency Contacts

The Agency Contacts information shows the details of the up to three contacts configured for each agency in the Agency Editor. These include each contact's name, email address, phone number and fax number.

The contact titles reflect those configured on the Preferences tab of the Site Administration page.

The following screenshot shows an example of the information:



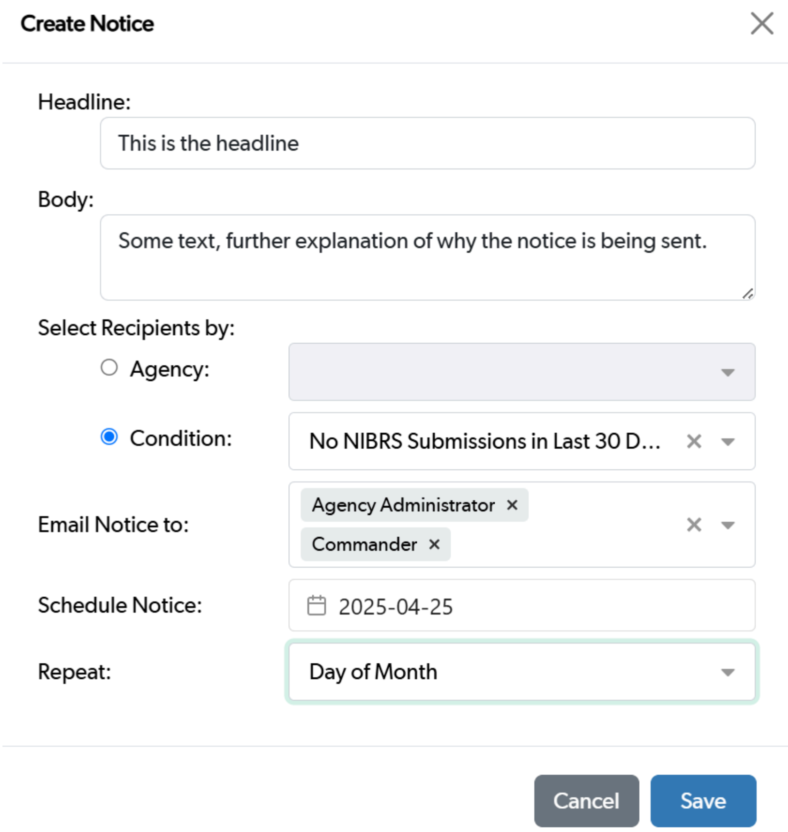
Notices

The Notices functionality allows for one-way communication from the State to agencies in the state. Users with access can send a notice to one or more agencies, including a brief subject line and more extensive text. Notices can be scheduled to run on a future date, either once or with a regular repeat. Crime Insight sends notices once per day, typically around 6:00PM, although Beyond 20/20 can configure this time to meet any state's requirements.

One key feature of a notice is that it can be set up to be sent to one or more specific agencies or to all agencies that meet a specific condition (e.g. failing to submit NIBRS data or failing to correct outstanding errors). As new data collections and functionality are added to Crime Insight, it is expected that the list of conditions will grow to meet the scenarios that are most important.

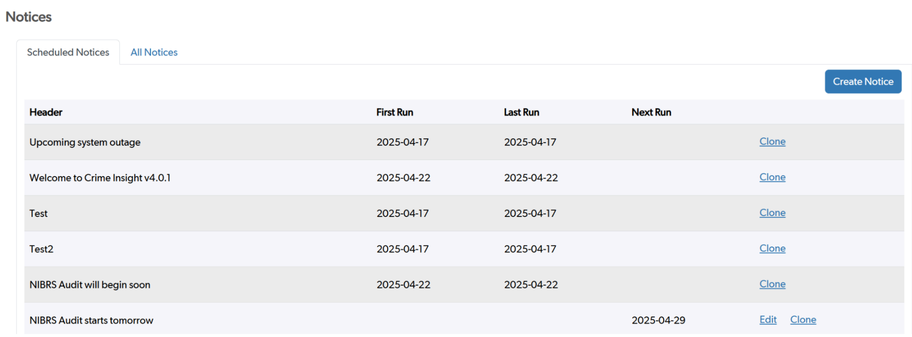
Another feature of notices is that they can also be sent as an email to one or more contacts at each agency. In the Agency Editor, it is possible to define up to three contacts for each agency. The names for the three contact types can be configured on the Preferences tab of the Site Administration page. When creating a notice, you can select one or more of these contact types. When the notice is delivered to an agency, an email is sent to the email address associated with the contact type in the Agency Editor.

Notices are available from the "Agency Communication" menu. The following screenshot shows the dialog box for creating a new Notice:



State users can see a list of all notices that have been set up, including those that have already been sent and those that are scheduled to be sent. Both State and agency users can see a list of delivered notices. Note that a notice that has been scheduled to repeat will appear once in the scheduled notices list, but multiple times (one for each run) in the Delivered Notices list. Of course, agencies can only see notices delivered to them.

The following screenshot shows an example of the list of scheduled notices:

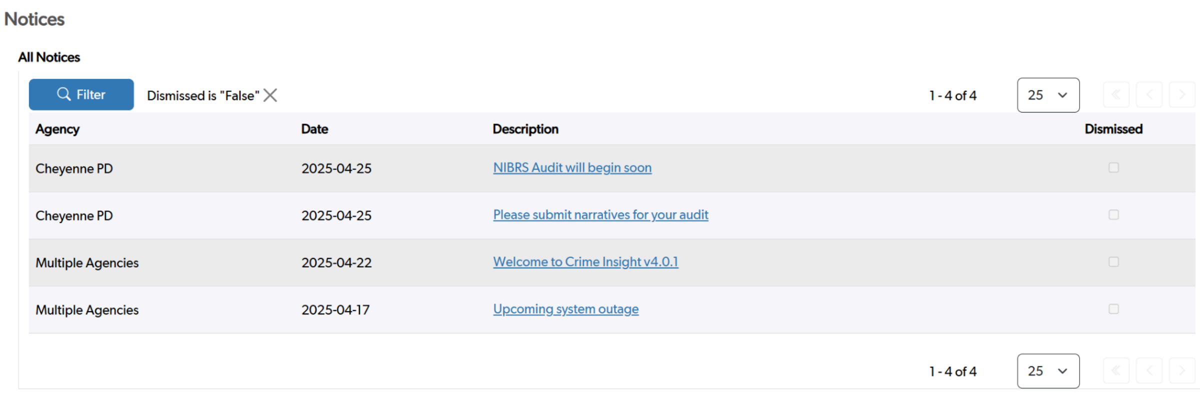

Notices

Scheduled Notices | All Notices

Create Notice

Header	First Run	Last Run	Next Run	
Upcoming system outage	2025-04-17	2025-04-17		Clone
Welcome to Crime Insight v4.0.1	2025-04-22	2025-04-22		Clone
Test	2025-04-17	2025-04-17		Clone
Test2	2025-04-17	2025-04-17		Clone
NIBRS Audit will begin soon	2025-04-22	2025-04-22		Clone
NIBRS Audit starts tomorrow			2025-04-29	Edit Clone

The following screenshot shows an example of the list of delivered notices for a single agency:


Notices

All Notices

Filter | Dismissed is "False" | 1 - 4 of 4 | 25

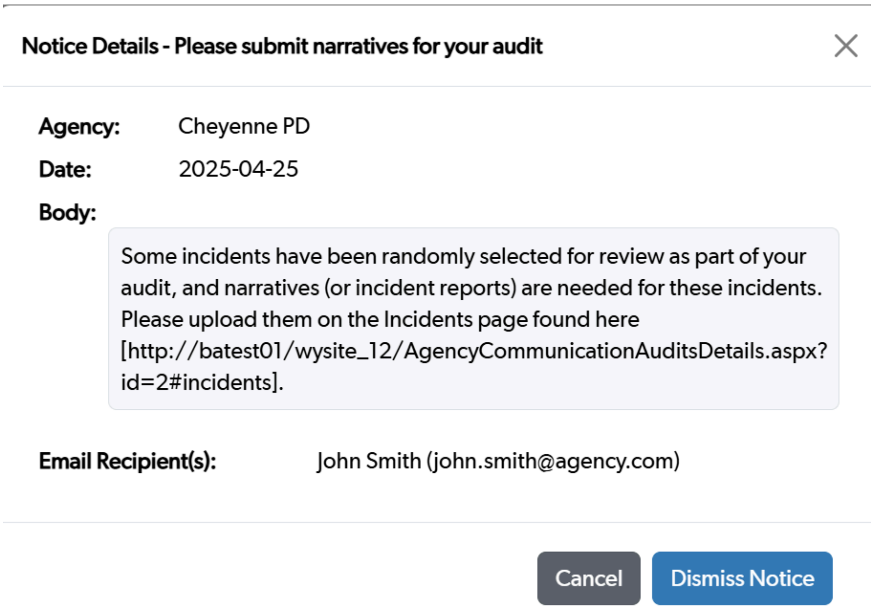
Agency	Date	Description	Dismissed
Cheyenne PD	2025-04-25	NIBRS Audit will begin soon	
Cheyenne PD	2025-04-25	Please submit narratives for your audit	
Multiple Agencies	2025-04-22	Welcome to Crime Insight v4.0.1	
Multiple Agencies	2025-04-17	Upcoming system outage	

1 - 4 of 4 | 25

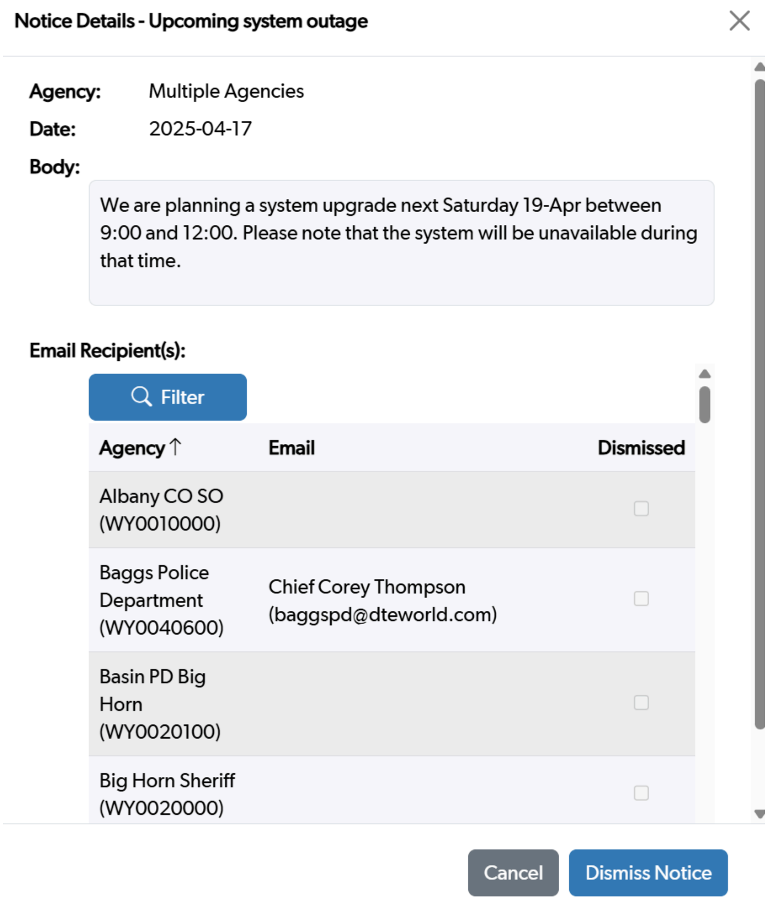
Once a notice has been delivered to an agency, it appears on the Agency Dashboard and on the Delivered Notices list until any user at the agency or at the State dismisses it. When an agency user dismisses a notice, it is dismissed for all users at the agency. When a State user dismisses a notice, it is dismissed for all agencies it was sent to. A typical example of when this would be useful is the case of a notice for a planned outage. After the outage is complete, there is no need for agencies to be aware of it any more, so it makes sense to dismiss the notice for all agencies.

Users can dismiss notices on the Notice Details page.

The following screenshot shows an example of the Notice Details page, as shown to a single agency:



The following screenshot shows an example of the Notice Details page for a State user:



Known Issues

The Notices functionality is being released with a small number of known issues. These are listed here for full transparency, and will be fixed in v4.0.2 or v4.0.3:

- When a daily or weekly notice is saved, it is saved with no schedule date. A daily notice will start running from tomorrow and a weekly one from next week
- Agencies who dismiss notices do not appear in the list of recipients on the Notice Details page.
- When an agency accesses the Notice Details page from the Notices page, the email recipients are not shown properly
- The Scheduled Notices tab is not shown in a reasonable order
- Filtering on the All Notices tab is not working

Audit

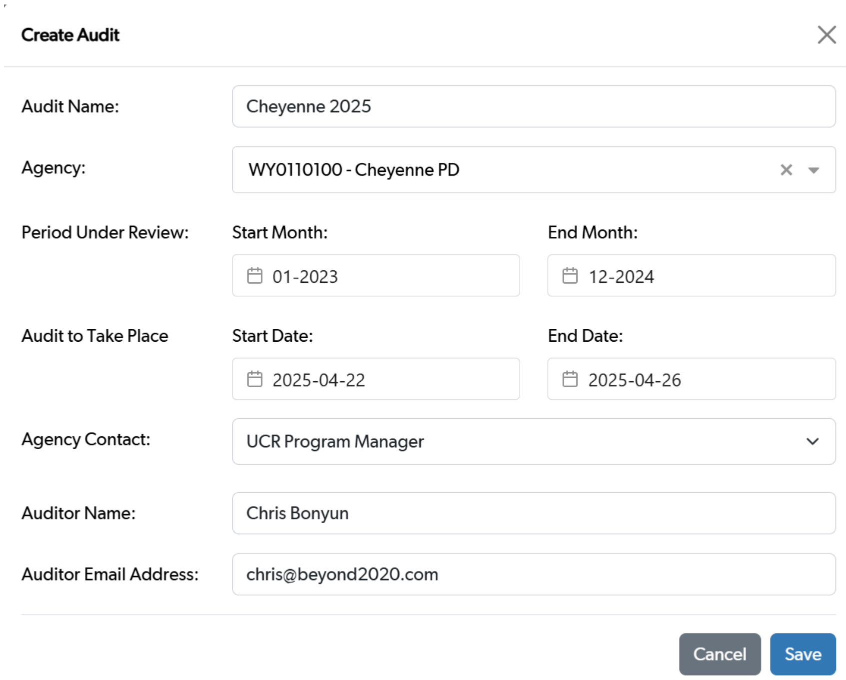
The Crime Insight Audit module provides support for states who wish to conduct audits on agencies' NIBRS submissions. An audit consists of the following key elements:

a) The auditor requests and reviews specific documents from the agency, with the option to include a blank template or questionnaire as the starting point.
b) The auditor asks Crime Insight to randomly select incidents for audit, based on selection criteria.
c) The agency uploads narratives for the selected incidents, so the auditor can compare the narrative to the submitted NIBRS data.
d) The auditor provides feedback on an incident-by-incident basis as well as a final report encompassing all of the findings.
e) Notices are sent throughout the process to keep the agency informed of expectations.
f) A continuous dialogue is encouraged between the auditor and the agency.
g) Uploaded documents and narratives are kept secure and will be automatically deleted after the audit is complete.

The process begins when a state user (auditor) creates a new audit. At this time, the auditor provides:

- A name for the audit
- The agency being audited
- When the audit will take place
- The period of time being reviewed in the audit
- An optional contact at the agency to receive email notifications about the audit
- Contact information for the auditor, in case the agency needs to reach them directly.

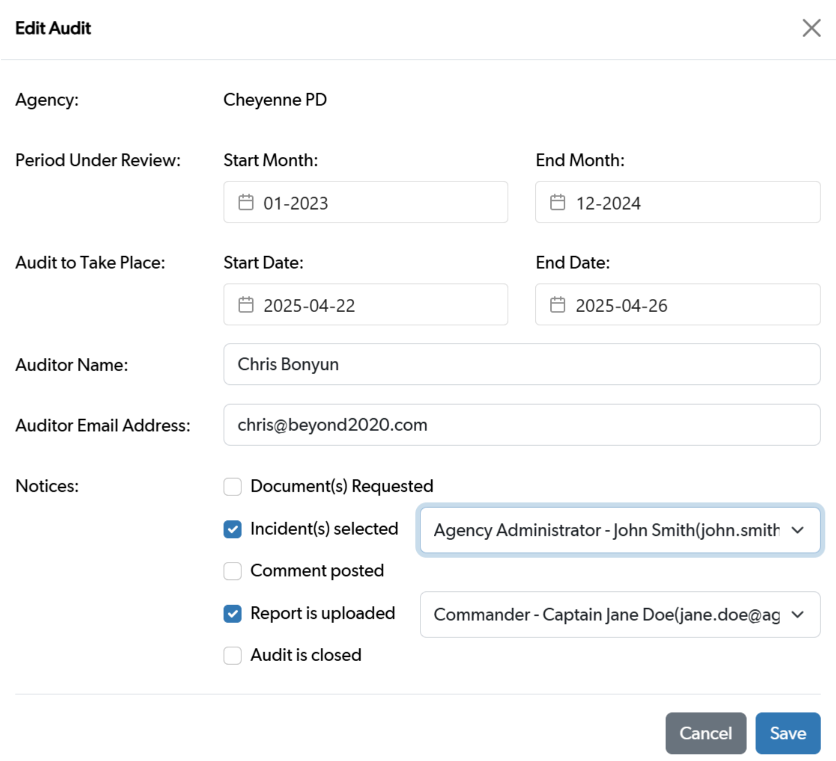
The following screenshot shows the screen to create an audit:



Once an audit is created, it appears in a table of all audits. The audits are shown with status and progress information. Entitled agency users can see the same page, but will only see audits for their own agency.

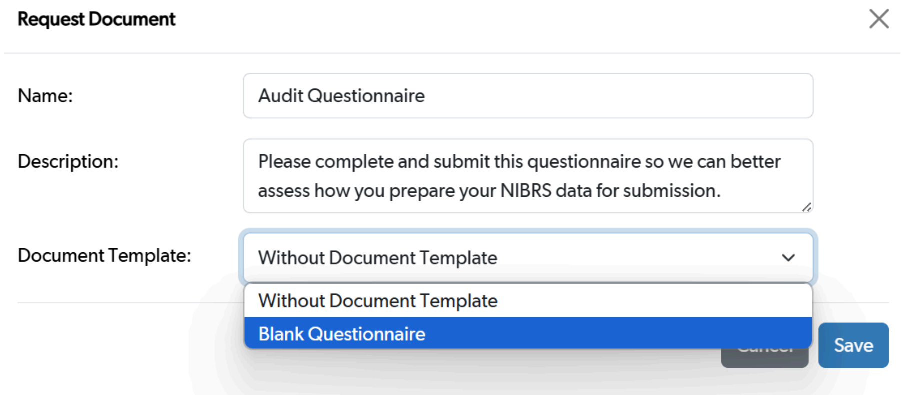
Clicking on any audit name brings up the Audit Details page, which shows the general information about the audit. This information can be edited by the auditor.

A key feature of editing an audit is that the auditor can control which events in the audit process create notices, and which of those notices also result in an email in addition to the on-screen delivery. The following screenshot shows the way in which this is controlled:



The second tab on the Audit Details page is the place where the auditor requests documents from the agency. A document can be requested by name/description (e.g. “any document describing your standard operating procedures”). In addition, a document template, such as a blank questionnaire, can be provided with the expectation that the agency will fill in the details and upload the completed document.

The following screenshot shows the dialog where the auditor requests a document to be uploaded:

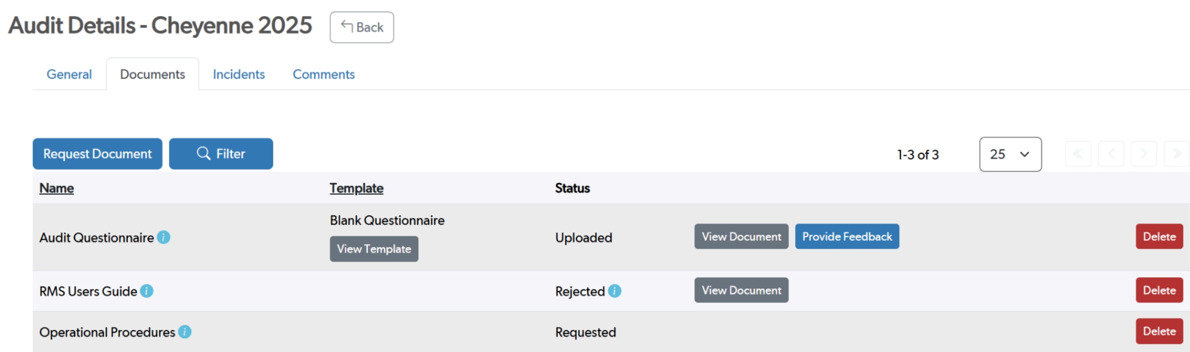


Document templates are managed on the “Document Templates” page, accessed from the “Agency Communication” menu. This page is very simple, allowing entitled users to upload and manage the templates to be used in the audit.

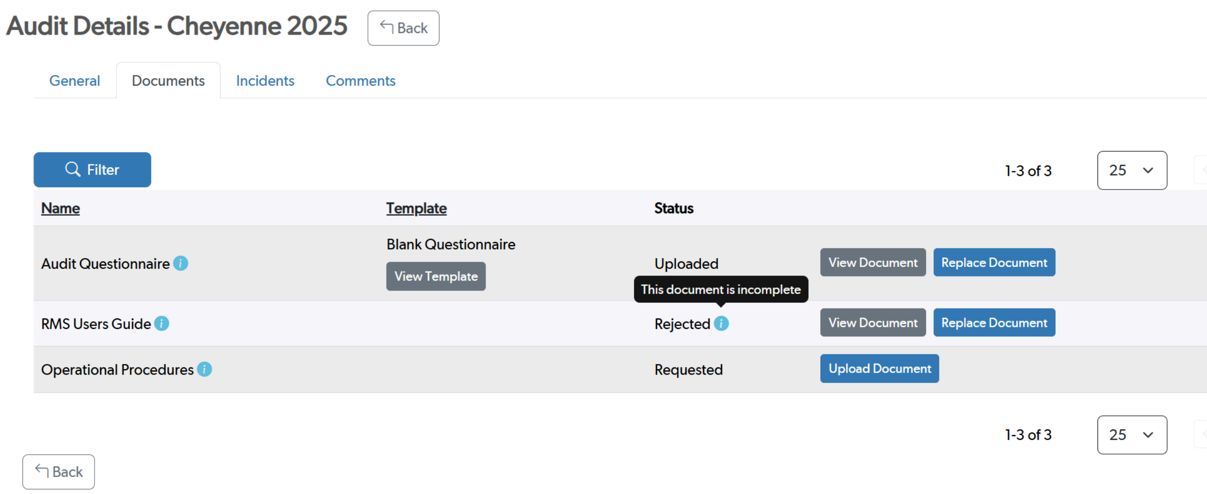
When the agency navigates to the Documents tab, they are shown the list of requested documents. For each document, the agency can click the Upload button to provide the requested information.

Once documents have been uploaded, the auditor can view them by clicking on the View Document button. The auditor has the option of accepting or rejecting each document. A document may be rejected, for example, if the agency accidentally uploads the wrong document, or if it is missing key information.

The following screenshot shows an example of the document list with documents in various states, as seen by the ***auditor***:



The following screenshot shows an example of the document list with documents in various states, as seen by the ***agency***:

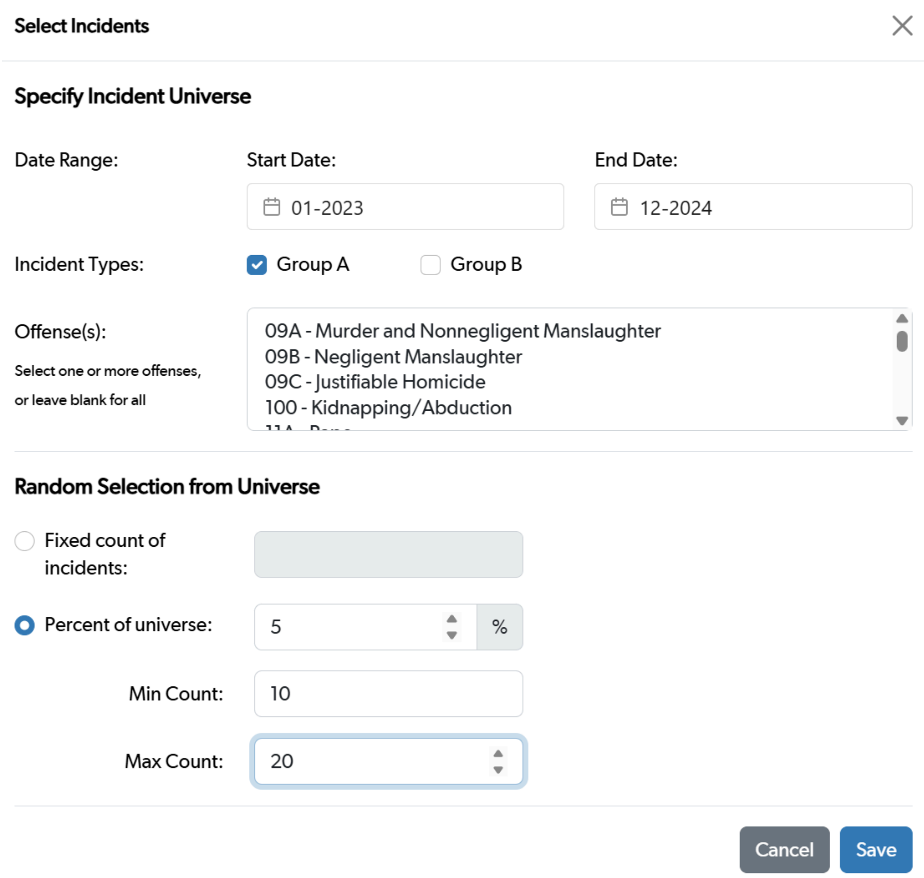


The third tab of the Audit Details page is where the auditor selects incidents and the agency provides narratives for the audit process. Incidents are randomly selected based on two key aspects:

1. The universe of incidents from which to make the selection
2. The size of the selection.

The universe is specified based on incident type (Group A or B), offense type(s), and the date of the incident (Group A) or arrest (Group B). The size of the selection is specified either as a simple count of records or a percentage of the universe.

The following screenshot shows an example of specifying a random incident selection:



When the selection settings are saved, a new job is triggered to find the incidents. An audit may include multiple jobs. For example, there may be a requirement to audit at least one murder (if any were reported by the agency), at least one drug crime, and a total of 20 from other Group A incidents. This would be specified in three different jobs (one for the murder, one for the drug crime, and one for all other Group A offenses).

The table at the top of the Incidents page shows all jobs created for the Audit. As each job runs, and incidents are selected, they appear in the lower table, which is visible to agency users as well as the auditor.

The incident list tracks the status of each incident, and:

- Allows/encourages agencies to upload a narrative for each selected incident.
- Allows both the agency and the auditor to view the Single Incident Viewer report for each incident (click on the incident number)
- Allows the auditor to view the uploaded narrative.
- Allows the auditor to reject the narrative (e.g., the wrong document, or it doesn't include enough information).
- Allows the auditor to provide feedback on each incident, having compared the submitted NIBRS data to the actual event.

The following screenshot shows an example of the incident list with incidents in various states, as seen by the ***auditor***:

Incidents

Filter 1-25 of 30 25

Incident Number	Type	Incident/Arrest Date	Status	
202400051597	A	2024-09-17	Narrative Rejected	View Narrative, Delete Request
202400015398	A	2024-03-22	Passed	View Narrative, Update Review, Delete Request
202300061716	A	2023-10-15	Failed	View Narrative, Update Review, Delete Request
202400019836	A	2024-04-15	Narrative Uploaded	View Narrative, Reject Narrative, Review Incident, Delete Request
202400003555	A	2024-01-20	Narrative Uploaded	View Narrative, Reject Narrative, Review Incident, Delete Request
202400037989	A	2024-07-01	Narrative Requested	Delete Request
202400014919	A	2024-03-20	Narrative Requested	Delete Request

The following screenshot shows an example of the incident list with incidents in various states, as seen by the ***agency***:

Incidents

Filter 1-25 of 30 25

Incident Number	Type	Incident/Arrest Date	Status	
202400051597	A	2024-09-17	Narrative Rejected	View Narrative, Replace Narrative
202400015398	A	2024-03-22	Passed	View Narrative, Replace Narrative
202300061716	A	2023-10-15	Failed	View Narrative, Replace Narrative
202400019836	A	2024-04-15	Narrative Uploaded	View Narrative, Replace Narrative
202400003555	A	2024-01-20	Narrative Uploaded	View Narrative, Replace Narrative
202400037989	A	2024-07-01	Narrative Requested	Upload Narrative
202400014919	A	2024-03-20	Narrative Requested	Upload Narrative

The last tab on the Audit Details page is for communication between the auditor and the agency. Anyone with access to the audit can enter a message. The full history of the dialog is kept in the audit, so it's possible to go back. Typical scenarios where this may be used would be when the agency has questions about the findings for a specific incident, or if the auditor wants clarification on any document uploaded by the agency.

Known Issues

The Audit functionality is being released with a small number of known issues. These are listed here for full transparency, and will be fixed in v4.0.3:

- Sort and Filter on some tables needs some cleaning up
- Closing an audit should stop all further updates
- Double-clicking on certain submit buttons results in the action being done twice
- Some recent Group B incidents are not included in the random incident selection
- The lifetime of uploaded narratives is not yet configurable -- set to a fixed 30 days from the time the audit is closed
- When an incident is selected in multiple selection jobs, it appears multiple times in the incident list -- should only be once

Web Service for Agency Submissions (TN Only)

Crime Insight now includes a new version of CI-API, the web service interface to Crime Insight, supporting NIBRS submissions in Tennessee. RMS systems in the state now have access to submit data automatically to Crime Insight without additional manual work by the agency. Of course, some software development will be needed to update the RMS to take advantage of this feature.

The general approach is that the RMS asks CI-API to validate each incident as it is being entered by the officer or records clerk. Then, on a regular schedule (weekly, daily, or more frequently as desired), the RMS submits all valid incidents to Crime Insight.

The advantages of this approach are:

1) The user gets feedback as they are entering the data, thus giving immediate feedback when the incident is still fresh in their mind.
2) The validation is guaranteed to reflect the state-level validation, so there will not be any surprises when the incidents are actually submitted.
3) There is no need for state staff to download/upload files. The submission is completely transparent to the user.

In order to make this work, the following steps are needed:

1. RMS is updated to take advantage of the web service.
2. Test system is updated to accept automated submissions for an agency, and a key is generated.
3. Key and connection information are provided to the RMS provider to set up in their system.
4. RMS provider tests the system with the Tennessee test environment.
5. Likely the state will want to recertify each agency.
6. Production system is configured to accept automated submissions for the agency and a new key is generated.
7. RMS is updated in production with the connection details and key.
8. Data starts flowing through to Crime Insight.

Domestic Violence in CO Cubes

In CO, as in several other states, there is a TOPS theme for Domestic Violence (DV). This theme performs very badly, with several charts not showing up on the first try. The root cause of the problem is that DV is defined as a specific group of offenses when the victim is related to the offender with specific relationship types. This requires special aggregation on the existing Offense Type and Relationship dimensions.

In v4.0.1, the CO Victim Cube has been extended to have two new dimensions, one for DV Offenses and another for DV Relationships. These two new dimensions can be used to make DV-related queries perform much faster. The CO TOPS DV theme will be updated to use the new dimensions, with expected improvements in performance.

Once this approach has been proven, we will adopt the same change in other states. Specifically, the MO cubes and TOPS will get the same treatment in v4.0.2.

Bug Fixes - Repository and Reporting

The following issues have been addressed in this release:

Who	ID	Description
All states	SUP-1153	Reduced the number of application errors (Error 500) seen on login.
All states	CI-2742	Improved activity tracking in the Incident Editor to reduce the likelihood of a session timeout and data loss.
All states	CI-2727	A 'contains' filter with a long criterion no longer interferes with the resulting file count.
All states	CI-2726	Corrected the NaN that was showing in the count of tasks on the Tasks page.
All states	CI-2724	Fixed some filtering issues related to removing criteria when more than one criteria is specified.
All states	CI-2717, 2718, 2719	Cleaned up some minor filtering issues.
All states	CI-2714	The new ORI column (in addition to the original Agency column) on the Errors & Warnings page is now hidden for users with access to a single ORI.
All states	CI-2706	When 20 files are selected for upload, the message that appears now indicates that any additional files must be uploaded in a subsequent upload.
All states	CI-2689	On the Upload pages of the various data collections, only files with appropriate extensions are accepted and the icons displayed beside the file name have been rationalized.
All states	SUP-1174	In some states, corrected the issue where the Incident Editor was throwing an error when trying to edit an accepted incident with drugs and property loss type = None.
All states	PER-129	You can now email the report definition of a microdata report.
All states	SUP-1209	Fixed an issue with the Password Recovery functionality in Perspective.
All UoF states	SUP-1162	A NIBRS incident that is submitted with the same ORI and incident number as a Use of Force incident no longer clears any errors from that Use of Force incident.
All UoF states	CI-2784	Unresolved Use of Force errors no longer interfere with NIBRS incidents displaying in the Incident Editor when the ORI and incident number are the same between the two datasets.
All UoF states	CI-2725	Ensured that any Use of Force errors or warnings appear at the top of the Use of Force editor, regardless of how you get to the editor.
All UoF states	CI-2729	The LEA role associated with the Use of Force cubes is now being correctly applied to all three Jurisdiction dimensions to ensure that a non-administrator user can only see data for their selected agencies when

		the data has been restricted by agency.
CO	SUP-1211	It is now possible to edit a contact and set the weapon discharged to false.
CO, ND, TN	SUP-1157	Downloading an old FBI file no longer affects the counts of incidents on the System Dashboard that are going to the FBI.
CO, ND, TN	CI-2836	Updated the FBI Web Service to ensure that all incident numbers and arrest transaction numbers are submitted to the FBI in upper case.
CO, NE	SUP-1181 SUP-1197	The Single Incident Viewer report now only shows current errors at the top of the report as opposed to all errors over the history of the incident.
CT, MO	SUP-1206	The Group A Single Incident Viewer report now shows the latest version of an incident when a valid incident is updated with a version with errors.
NE	NE-403	The Age Suitable for Banding dimension has been removed from the state-specific All Arrestee Data cube.
NH, ME, MS	SUP-1192	The Single Incident Viewer now shows the latest instance of an incident as opposed to the last upload without error.
NV	SUP-1180	Improved the performance of the Incident Editor that was sometimes producing an error page due to a timeout.
TN	TN-368, TN-579	The Age Suitable for Banding dimension has been removed from the state-specific (ss) All Arrestee Data cube, the ss Group B Arrestee cube and the ss Offender Data cube.
TN	SUP-1198	The Single Incident Viewer no longer reports, at the top of the report, that there is an accepted version of the incident when there is not.
TN	SUP-1164	Performance has been greatly improved for the Single Incident Viewer and Incident Lifecycle reports.
TN, VA	CI-2716	The ORI dropdown on the Use of Force Single Incident Viewer report now shows a sorted list of agency names and ORIs.
VA	VA-470	Failed Community Policing uploads now appear correctly in any filter result that should return Failed submissions.
VA	SUP-1161	When there are no stolen or recovered vehicles in an incident, the microdata now displays a blank instead of -1.