



### Secured Incident Access Enhancements

A series of new features have been added to the handling of secured incidents that have an intelligence level assigned. These additions will provide for simpler management of secured incidents, more auditing capability, and easier access for officers involved.

#### Officers Can View Assigned Secured Incidents

The currently assigned officer of a secured incident will be allowed to access the incident. This will happen regardless of the officer's level of access to incidents at the particular security level. In other words the assigned officer will be allowed to view a secured incident he is not otherwise normally able to view. This is designed to permit the officer to be able to more easily work on the secured incident assigned to him/her. This in no way extends the officer's ability to view other incidents secured at the same level. It only applies to the incidents the officer is in charge of. Other involved officers do not gain this special status, it only applies to the officer in charge.

#### Access to Secured Incidents is Logged

Each time a secured incident is accessed for either inquiry or maintenance, a log entry will be made in the incident activity log. This will keep a detailed log of all personnel that have accessed or tried to access sensitive incidents that have been secured. This feature is not affected by what type of security level is used. Any security level assigned to an incident will cause this extended logging of access to the incident. If the person is authorized to view the particular security level, the log entry will state they viewed the incident. If the person is not authorized to view the incident, the log entry will state they were denied access. Both types of log entries are also generated by access from the MDC. Examples of the log entries can be seen in the figure below.

INCIDENT ACTIVITY LOG - List View IRMI305R

Order: \*ASCEND

Date/Time   to   Acty ID

User  Group  Type  Reference

Options:

Opt	Date/Time	Description	User
<input type="checkbox"/>	12/02/2004 15:11	Access to secured incident 940000002 denied	CRIMETEST
<input type="checkbox"/>	12/02/2004 15:11	Access to secured incident 940000002 denied	CRIMETEST
<input type="checkbox"/>	12/02/2004 19:13	Access to secured incident 940000002 denied	QPGMR
<input type="checkbox"/>	12/13/2004 1:36	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:48	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:54	Secured incident 040000003 viewed-confirmed	CRIMETEST2

## C.R.I.M.E. Release Announcement Letter

### Security Levels Available

As shown in the table below there are currently four security levels with three of them intended to be used in a hierarchy of varying sensitivity of the incident. These would range from minor incident security needs limiting access to just the involved agency, up to internal investigations that require more stringent measures. The fourth level was intended for use with MEG units and their cases. The extended level of logging will aid the MEG units and others in keeping a lid on information flow regarding sensitive cases. Keep in mind that any access granted to an officer or other personnel to a particular security level only applies to your agency. In other words if the supervisor from agency ANYTOWN grants officer 100 access to level 3, it is only level 3 for ANYTOWN's incidents. Officer 100 cannot view a level 3 incident owned by BIGCITY agency.

Level	Description
M	MEG Unit Access
3	Limited Access
5	Restricted Access
7	Highly Restricted Access

### Notification Upon Entering a Secured Incident

When a person attempts to view or maintain a secured incident, a confirmation window will appear explaining that they are about to enter a secured incident. The text in the popup window is intended to warn those who have access to the particular security level to use it properly. Upon receiving the confirmation window, a choice must be made to either continue on and view the incident or exit without viewing the incident. Either action results in a log entry being created. The log entry will show the choice made. The recipient of this popup window is acknowledging they are aware this incident has been secured. An example of the popup window is displayed below.



### C.R.I.M.E. Release Announcement Letter

In the example screen below you can see at the bottom of the list examples of the two types of messages that could be written to the log. The first showing the decision to view the secured incident, and the second showing the decision to exit before viewing the incident. In an effort to not build road blocks to staff getting their work done, subsequent attempts to view the same incident after having viewed it before will not cause the popup window to appear. However, viewing a different incident in between attempts to view the same incident will cause the popup window to re-appear.

The screenshot displays the 'INCIDENT ACTIVITY LOG - List View' interface. At the top, there is a menu bar with icons and the text 'ATN ENT HLP PRT RST SRQ'. Below this, the title 'INCIDENT ACTIVITY LOG - List View' is centered, and 'IRMI305R' and 'Order: \*ASCEND' are on the right. A search section contains fields for 'Date/Time' (11/05/2004 0:00:00 to 12/31/2099 24:00:00), 'Acty ID', 'User', 'Group', 'Type', and 'Reference'. An 'Options:' section has a button for 'P=Print Entry Detail'. The main area is a table with columns: Opt, Date/Time, Description, and User. Below the table are buttons for 'F3=Exit', 'F5=Refresh list', 'F10=Document View', and 'F11=Activity Detail'. The bottom right corner shows 'Row: 4 Col: 12'.

Opt	Date/Time	Description	User
<input type="checkbox"/>	12/02/2004 15:11	Access to secured incident 940000002 denied	CRIMETEST
<input type="checkbox"/>	12/02/2004 15:11	Access to secured incident 940000002 denied	CRIMETEST
<input type="checkbox"/>	12/02/2004 19:13	Access to secured incident 940000002 denied	QPGMR
<input type="checkbox"/>	12/13/2004 1:36	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:48	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:54	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:54	Exited before viewing secured incident 040000003	CRIMETEST2
<input type="checkbox"/>	12/13/2004 1:58	Exit before viewing secured incident 040000003	CRIMETEST2
<input type="checkbox"/>	12/14/2004 14:43	Service ACCIDENT changed	CRIME
<input type="checkbox"/>	12/14/2004 23:38	Secured incident 040000003 viewed-confirmed	CRIMETEST2
<input type="checkbox"/>	12/14/2004 23:39	Exit before viewing secured incident 040000003	CRIMETE +

## C.R.I.M.E. Release Announcement Letter

### Searching for Access Attempts

Obviously, to view the activity for a specific incident, simply go into the Incident Activity Log from within the incident, which will show only the entries relevant to the incident. As an audit measure, to view all attempts to access secured incidents, go into the Incident Activity Log from the menu (no specific incident used), and use the search criteria TYPE with a code of "SECUR". Alter the date range as necessary and this will present a list of all attempts to view secured incidents and changes to the security level. Below is an example screen that shows when the security level was set and various attempts to access the incident.

**INCIDENT ACTIVITY LOG - List View** IRMI305R  
Order: \*DESCEND

Date/Time   to   Acty ID

User  Group  Type  Reference

Options:

Opt	Date/Time	Description	User
<input type="checkbox"/>	10/15/2004 10:12	Service ACCIDENT security changed	CRIME
<input type="checkbox"/>	10/15/2004 19:42	Secured incident 040000003 viewed	CRIMETEST2
<input type="checkbox"/>	10/15/2004 19:42	Access to secured incident 040000003 denied	CRIMETEST2
<input type="checkbox"/>	10/15/2004 19:42	Access to secured incident 040000003 denied	CRIMETEST2
<input type="checkbox"/>	10/15/2004 19:42	Access to secured incident 040000003 denied	CRIMETEST2
<input type="checkbox"/>	10/15/2004 19:42	Access to secured incident 040000003 denied	CRIMETEST2
<input type="checkbox"/>	10/15/2004 19:42	Access to secured incident 040000003 denied	CRIMETEST2
<input type="checkbox"/>	10/16/2004 10:01	Secured incident 040000003 viewed	CRIMETEST2
<input type="checkbox"/>	10/22/2004 12:39	Access to secured incident 040000003 denied	QPGMR
<input type="checkbox"/>	10/22/2004 15:15	Access to secured incident 040000003 denied	QPGMR
<input type="checkbox"/>	12/13/2004 1:36	Secured incident 040000003 viewed-confirmed	CRIMETE +