

**Oracle® Fusion Middleware**  
User's Guide for Oracle Public Sector  
Incident Reporting Process Accelerator  
11gRelease 1 (11.1.1.7.1)

January 2014

**ORACLE®**

**Copyright © 2012, 2014, Oracle and/or its affiliates. All rights reserved.**

### **Disclaimer**

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

### **Restricted Rights Notice**

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

#### **U.S. GOVERNMENT RIGHTS**

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

### **Trademark Notice**

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

---

# CONTENTS

<b>Oracle Public Sector Incident Reporting Process Accelerator .....</b>	<b>1</b>
What's New in this Release 11.1.1.7.1 .....	3
Overview of Oracle Process Accelerators .....	4
Getting Started with Oracle Public Sector Incident Reporting .....	7
Overview of Oracle Public Sector Incident Reporting Process Lifecycle .....	7
Email Notification Lifecycle .....	10
Understanding Oracle Public Sector Incident Reporting Pages .....	11
Starting Oracle Public Sector Incident Reporting .....	12
Using Oracle Public Sector Incident Reporting .....	13
Submitting an Incident Report .....	13
Reviewing an Incident Report .....	19
Assessing an Incident Report .....	21
Evaluating an Incident Report .....	23
Updating an Incident Report .....	24
Assigning a Responder to an Incident Report .....	26
Associating Related Incident Reports .....	28
Withdrawing an Incident Report .....	29
Closing an Incident Report .....	31
Searching Incidents by Person .....	33
Analyzing Incidents .....	34
Viewing NIEM Documents for an Incident Report .....	36
Administering Oracle Public Sector Incident Reporting .....	39
Maintaining Oracle Public Sector Incident Reporting Drop-down Lists .....	39
Maintaining Lookup Type Codes .....	39
Maintaining Responders .....	43
Maintaining Jurisdiction Access .....	46
Maintaining Global Lookup Type Codes .....	48
Maintaining Country Codes .....	51
Maintaining State Codes .....	53
Understanding Oracle Public Sector Incident Reporting Business Rules .....	57
Understanding the Determine Incident Type Priority Ruleset .....	58
Understanding the Determine Location Type Priority Ruleset .....	58
Understanding the Calculate Incident Priority Ruleset .....	59
Understanding the Search Similar Incidents Ruleset .....	60
Understanding the Compare Incident Threshold Ruleset .....	61
Understanding the Get Approvers Ruleset .....	61
Understanding Oracle Public Sector Incident Reporting Reports .....	62
Delivered Documentation .....	68



# Oracle Public Sector Incident Reporting Process Accelerator

*Oracle Fusion Middleware User's Guide for Oracle Public Sector Incident Reporting Process Accelerator* describes how to administer and use this process accelerator.

## Audience

This document is intended for:

- Citizens and reporters who use Oracle Public Sector Incident Reporting to submit incident reports
- Case workers and other personnel who use Oracle Public Sector Incident Reporting to disposition incident reports
- Administrators who maintain Oracle Public Sector Incident Reporting drop-down lists, business rules, and reports

Within this guide, the term *disposition* means the ability of authorized personnel to approve, reject, or request a change to a submitted incident report.

## Related Documents

For more information, see the following Oracle resources:

Oracle Public Sector Incident Reporting Process Accelerator

- *Oracle Fusion Middleware Installation Guide for Oracle Process Accelerators*
- *Oracle Fusion Middleware Extensibility Guide for Oracle Process Accelerators*

Oracle Business Process Management Suite

- *Oracle Fusion Middleware User's Guide for Oracle Business Process Management*
- *Oracle Fusion Middleware Modeling and Implementation Guide for Oracle Business Process Management*
- *Oracle Fusion Middleware Business Process Composer User's Guide for Oracle Business Process Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*

Oracle Business Rules

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*

Oracle Fusion Middleware

- *Oracle Fusion Middleware Administrator's Guide*

## Conventions

The following text conventions are used in this document:

- **boldface** - Boldface type indicates graphical user interface elements, or terms defined in text.

- *italic* - Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

## What's New in this Release 11.1.1.7.1

For Release 11.1.1.7.1, this guide has been updated in several ways. The What's New diagram depicts the sections or topics that have been added or changed.

### What's New

<b>Sections / Topics</b>	<b>Changes Made</b>
<b>Understanding the Determine Incident Priority Ruleset</b>	Section updated with ruleset image for better understanding.
<b>Understanding the Location Type Priority Ruleset</b>	Section updated with ruleset image for better understanding.
<b>Understanding the Calculate Incident Priority Ruleset</b>	Section updated with ruleset image for better understanding.
<b>Understanding the Search Similar Ruleset</b>	Section updated with ruleset image for better understanding.
<b>Understanding the Compare Incident Threshold Ruleset</b>	Section updated with ruleset image for better understanding.
<b>Understanding the Get Approvers Ruleset</b>	Section updated with ruleset image for better understanding.

## Overview of Oracle Process Accelerators

### Introduction

Oracle Process Accelerators are process solutions, developed by Oracle, which address common business processes or high-value industry processes. Oracle Process Accelerators have been developed to simplify and improve the management of these processes. Many low-priority business processes, such as managing travel approvals, are managed manually or through email and can negatively impact organizations by contributing to inefficiency and reduced productivity. In addition, there are complex business processes, some common to all organizations, and others specific to a particular industry, which benefit from the process management approach which Oracle Business Process Management (BPM) provides. Automated process management solutions enable organizations to become more efficient, to meet business challenges rapidly and flexibly, and ultimately to improve customer satisfaction by supporting employees in fulfilling requirements in a timely fashion.

### Key Elements

Oracle Process Accelerators, developed with Oracle BPM Suite 11g, make the following capabilities available to organizations implementing automated solutions to improve process management:

- **Role-Based Employee Access** - Processes are performed by people in the organization who do the work. When the employees are assigned to roles in the Oracle Process Accelerator, they have access to only those tasks in a process for which they are responsible. Multiple employees can be assigned to a role. Any one of them can select a task to get the job done.
- **Sequenced Tasks** - The work to be done is defined as a sequence of tasks, each performed by a role. After a task is completed, the solution automatically moves on to the next task. This is referred to as *workflow*. The sequence of tasks can branch into two or more paths depending on the outcome of a previous task. Note that some tasks require employee or user interaction, while some are automated. User tasks can be as common as clicking a button to approve a request, or as specific as entering an order with multiple line items.
- **Automated Task Lists** - When an employee logs in to an Oracle Process Accelerator, he is presented with a task list containing the work assigned to all of the roles he is responsible for. By selecting a task, the employee is guided to the appropriate application form, which prompts for the correct actions to be performed. After the actions are complete, the task disappears from the task list, and a new task is created for the role responsible for the subsequent task.
- **Business Rules** - Oracle BPM provides flexible business rules which can be defined to meet organizational guidelines. These rules are defined to support a specific process, and govern the way the process is carried out. For example, in a specific process, a request for management approval might require two levels of approval if an employee is grade four or lower, but only one level if grade three or higher.
- **Process Dashboards** - A useful component of Oracle Process Accelerators is the process dashboard reporting developed with Oracle Business Activity Monitoring (BAM). These reports provide real time process analytics which can be used to observe key performance indicators, and to monitor the efficiency of the process itself.

### The Business Process Diagram

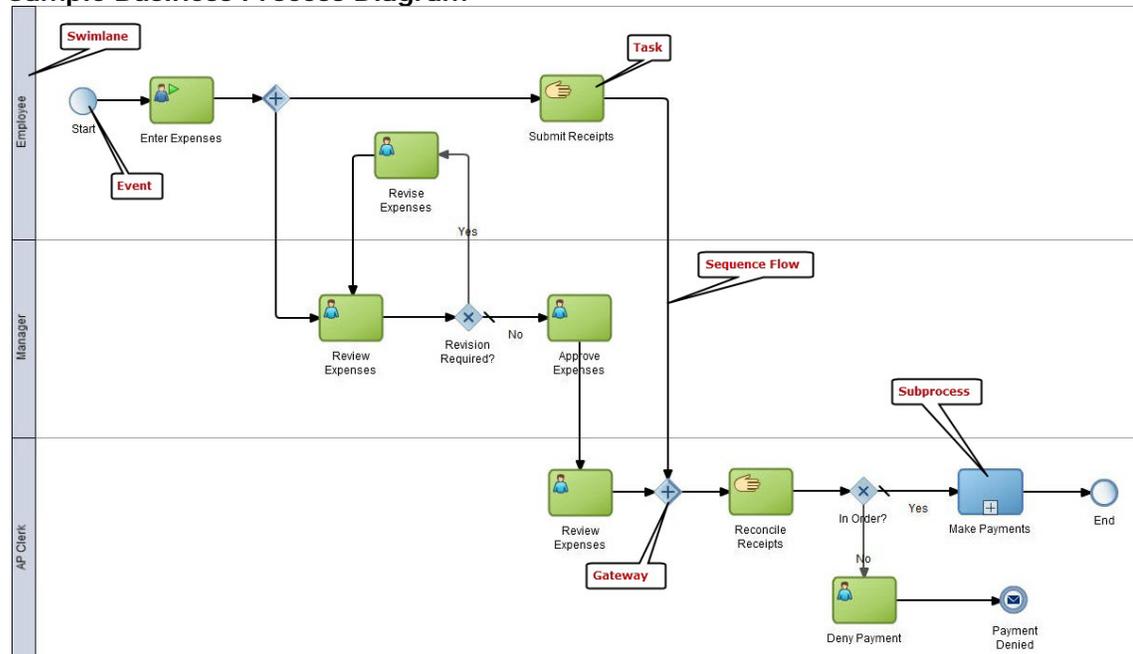
In the introduction to each Oracle Process Accelerator, a business process diagram shows the process being automated using the Business Process Modeling Notation (BPMN). For those unfamiliar with BPMN, the Sample Business Process Diagram provides an example.

The process diagram contains the following elements. If you are not familiar with this type of diagram, study the elements and then follow the diagram to understand the process.

- **Swimlanes** (Employee, Manager, AP Clerk) - contain roles that indicate who is responsible for the tasks in the lanes.
- **Events** (Start, End) - show where the process begins and ends.
- **Tasks** (Enter Expenses, Deny Payment) - identify the action being taken.
- **Sequence flows or arrows** - show the path to the next task.
- **Gateways** (Revision Required, In Order) - are diamond shapes indicating a branch in the path. In the sample diagram a parallel gateway (a + in the diamond), shows that both branches must be taken, and an exclusive gateway (an X in the diamond), indicates that only one path can be taken.
- **Subprocesses** (Make Payments) - indicate that another set of tasks has been collapsed for clarity.

For more information about BPMN, see "Overview of Business Process Design," in *Oracle Fusion Middleware Modeling and Implementation Guide for Oracle Business Process Management*.

### Sample Business Process Diagram



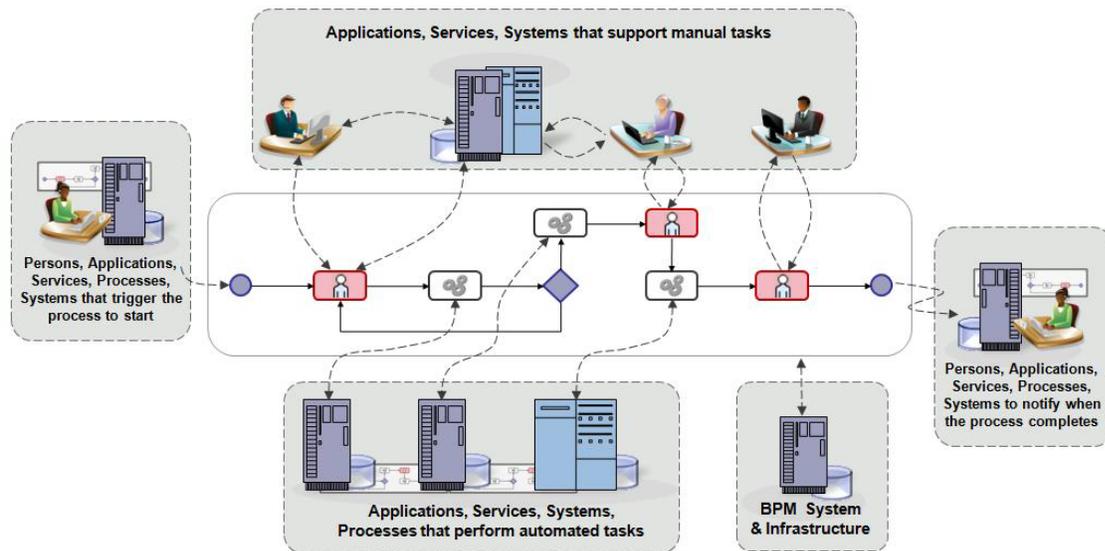
### Why Oracle Process Accelerators

An organization engaged in automating critical high-value processes with Oracle BPM Suite can benefit from the implementation of Oracle Process Accelerators. These pre-built solutions supplement the benefits of Oracle BPM Suite in these ways:

- **Consensus Building** - Using these pre-built processes, the IT organization can illustrate the advantages of process-driven applications, to show the value of process automation to the business community.
- **Best Practice** - A best practice guideline based on the accumulated experience and expertise of Oracle developers and implementers is provided with Oracle Process Accelerators. These best practices mitigate the risk associated with learning and deploying a new technology. The guide includes development methodologies, process modeling approaches, effective tool use techniques, and sample deployment plans. Oracle uses these best practices to build the Oracle Process Accelerators.

- **Rapid Deployment** - The Oracle Process Accelerators can be implemented as is or extended to meet specific requirements. In either scenario, there is a significant reduction of effort.
- **Build a Process Centric Organization** - Clearly, an organization will not be using Oracle BPM and Oracle Process Accelerators to computerize a small set of common business processes. It is highly likely that a critical value-add process that provides a market differentiation is being automated to improve customer satisfaction or reduce costs. While the more significant project is underway, the business community can start to learn how to use process driven applications to their benefit. By rolling out Oracle Process Accelerators, the organization gets a head start with the new paradigm. If multiple Oracle Process Accelerators are deployed, the management community begins to learn that process automation reduces the overhead associated with handling mundane tasks. The implementing organization has the opportunity to win a quick victory with the new technology, and the business users learn the value of managing tasks through accurately routed processes. The organization as a whole begins to appreciate the benefits of becoming process-centric. The Sample Functional Architecture for Oracle Process Accelerators diagram depicts how the Oracle Process Accelerators can be used in an organization.

### Sample Functional Architecture for Oracle Process Accelerators



## Getting Started with Oracle Public Sector Incident Reporting

This section is intended for new Oracle Public Sector Incident Management (PSIR) users who want a brief introduction.

Upon completion of this section, you will be able to:

- Describe the basic Oracle Public Sector Incident Reporting process lifecycle.
- Describe Oracle Public Sector Incident Reporting pages and related Oracle Business Process Management Workspace pages.
- Start Oracle Public Sector Incident Reporting.

## Overview of Oracle Public Sector Incident Reporting Process Lifecycle

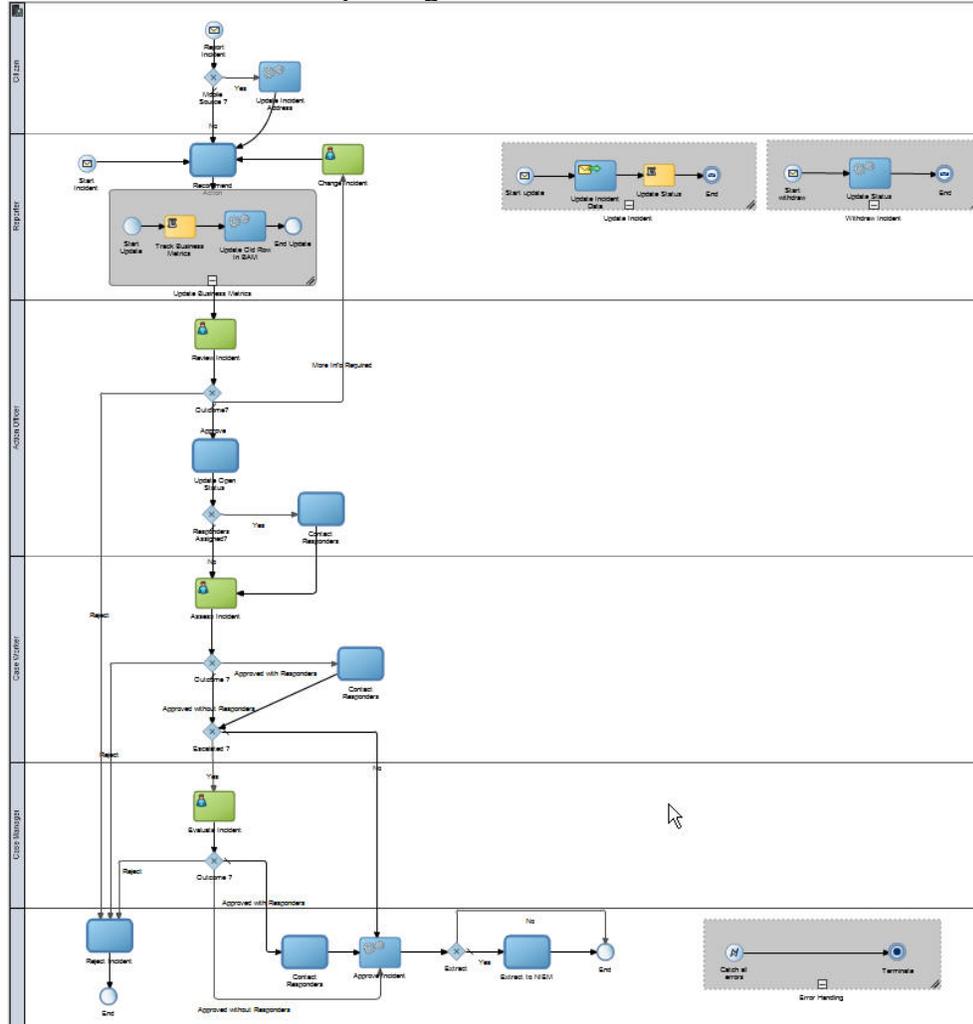
Oracle Public Sector Incident Reporting (PSIR) Process Accelerator is a process solution that enables public sector organizations to capture data about and respond to incidents. The types of incidents can be defined by the implementing organization. Oracle PSIR provides dashboards to view process analytics and incident request summary reports. Administrators can modify the business rules and the drop-down lists.

Oracle PSIR is a role-based solution; your role determines the tasks you can perform. Oracle PSIR delivers the following roles:

- The citizen is someone outside the implementing organization that submits an incident report through the mobile or web application.
- The reporter collects information about the incident and submits an incident report.
- The action officer reviews the incident report to ensure sufficient data is collected and assesses or assigns responders.
- The case worker reviews the incident report to determine if a higher level response is required.
- The case manager reviews the escalated incident reports.

The Incident Reporting Process is the main business process for Oracle PSIR, and the focus of this topic. Because Incident Reporting is a top-level process, it consists of inline and callable subprocesses. The Public Sector Incident Reporting Process diagram is depicted as follows, with an explanation of the process.

Public Sector Incident Reporting Process



The Public Sector Incident Reporting Process involves the following basic tasks:

1. The reporter or citizen submits an incident report.
2. If the incident report is submitted using a mobile device, then the Update Incident Address task translates the mobile device coordinates into the physical street address using Oracle Spatial Services.
3. An automated task evaluates the incident and recommends action as needed.
4. The action officer reviews the incident report to determine if additional information is required, or assigns local responders if needed and approves the incident report.
5. The case worker assesses the incident report to determine if additional responders are needed and associates related incidents. The case worker escalates the incident report if outside agency responders are required.
6. The case manager evaluates the incident report to determine if outside agency responders are needed. The case worker or the case manager can extract the incident report to a national information exchange (NIEM) model.

This topic walks through the Oracle Public Sector Incident Reporting Process illustrating how a reporter submits an incident report and personnel manage the incident report.

### ***Overview of Oracle Public Sector Incident Reporting Process Lifecycle***

1. The reporter or citizen begins by navigating to the **Enter Incident Report** page.
2. The reporter or citizen uses the **Enter Incident Report** page to create and submit an incident report.
3. The reporter or citizen completes all required fields pertaining to the incident.
4. The reporter or citizen completes all appropriate fields pertaining to the attacker, responder, suspect, victim, or witness.
5. The reporter or citizen completes all appropriate fields pertaining to the arson incident.
6. The reporter or citizen clicks the **Submit** button, to save and submit the incident report.
7. The action officer uses the **My Tasks** page to review incident reports.
8. The action officer double clicks the **Task** to open the incident report.
9. The action officer uses the **Review Incident** page to review the incident report and assign local responders.
10. The action officer clicks **Claim** to assign this task to himself if multiple action officers are presented with this task.
11. The action officer reviews the incident report and determines what local responder to assign.
12. The action officer adds a local responder to the incident report.
13. The action officer clicks the **Approve** button, which approves the incident report.
14. The case worker uses the **My Tasks** page to assess incident reports.
15. The case worker double clicks the **Task** object to open the incident report.
16. The case worker uses the **Assess Incident** page to assess the incident report and escalate the incident report to the case manager.
17. The case worker assesses the incident report and determines it needs to be escalated.
18. The case worker adds comments for the case manager.
19. The case worker clicks the **Escalate** button, which escalates the incident report.
20. The case manager uses the **My Tasks** page to evaluate incident reports.
21. The case manager double clicks the **Task** object to open the incident report.
22. The case manager uses the **Evaluate Incident** page to evaluate the incident report and add national and international responders.
23. The case manager evaluates the incident report and determines no more responders are needed.
24. The case manager clicks the **Approve** button to approve the incident report and extract it to a NIEM compliant document.

25. The case manager confirms to extract the incident report to a NIEM compliant document.
26. You have completed the **Overview of Oracle Public Sector Incident Reporting Process Accelerator Lifecycle** topic.

## Email Notification Lifecycle

As requests are submitted and move through each task of the process lifecycle, the responsible user for each task receives an email notification informing them of the actions they need to take. The email notifications are actionable. Actionable emails enable a user to disposition a request without logging in to the process accelerator. A reminder email notification is sent if a user does not disposition a request in a timely fashion.

The following scenario illustrates the email notification lifecycle.

Scenario: Jcooper submits a request. The reviewers and approvers, in sequence, are Jstein, Wfaulk, and Cdickens. Wfaulk delays approving the request and an email notification is sent.

1. Jcooper submits a request.

1a. Jcooper receives an email notification that the request is assigned to the action officer Jstein.

1b. Action officer Jstein receives an actionable email that the request is assigned to him. He can approve, request more details, or reject the request from either a web or mobile email client. Requests for details or rejections require comments to be added.

2. Jstein approves the request by clicking **Approve**.

2a. A new email is created when Jstein clicks **Approve**, then clicks **Send**.

2b. Jcooper receives an email notification that the request is assigned to case worker Wfaulk.

2c. Wfaulk receives an actionable email that the request is assigned to him.

3. Wfaulk does not respond to the email. After two days, a reminder notification email is triggered and sent to Wfaulk.

3a. Jcooper receives an email notification that the request is assigned to case worker Wfaulk.

3b. Wfaulk receives an actionable email that the request is assigned to him.

4. Finally Wfaulk approves the request.

4a. Jcooper receives an email notification that the request is assigned to case manager Cdickens.

4b. Cdickens receives an actionable email that the request is assigned to him.

5. Cdickens can approve or reject the request.

5a. If approved, Jcooper receives an email notification that his request is approved by the final approver in the hierarchy.

5b. If rejected, Jcooper receives an email notification that his request is rejected. Jcooper receives a rejection email notification when any approver rejects his request.

## Understanding Oracle Public Sector Incident Reporting Pages

Oracle Public Sector Incident Reporting (PSIR) runs on Oracle Business Process Management Workspace. Your role within Oracle PSIR determines the tasks you can perform and the pages you can access. Some of these pages are Oracle Business Process Management Workspace, others are Oracle PSIR. Understanding the pages associated to a task or role makes you more effective in your use of Oracle PSIR.

This topic addresses the various Oracle Business Process Management Workspace and Oracle PSIR pages you use.

### ***Understanding Oracle Public Sector Incident Reporting Pages***

1. The Oracle Business Process Workspace **Tasks** page appears after you log into Oracle Business Process Management Workspace. This is an Oracle Business Process Management Workspace page.  
  
From here you can:
  - Take action on an incident report by executing the tasks assigned to you in **Views, My Tasks**
  - Access Oracle PSIR from the **Applications** link
2. The **Report an Incident** link is visible if you are granted permissions in Oracle PSIR. Use this link to access the **Enter Incident Report** page. This is an Oracle Business Process Management Workspace page.
3. Use the **Enter Incident Report** page to create and submit an incident report. This is an Oracle Public Sector Incident Reporting page.
4. Use the **Review Incident** page to review the incident report and add local responders. This is an Oracle Public Sector Incident Reporting page.
5. Use the **Assess Incident** page to assess the incident report and add local responders. This is an Oracle Public Sector Incident Reporting page.
6. Use the **Evaluate Incident** page to evaluate the incident report and add national and international responders. This is an Oracle Public Sector Incident Reporting page.
7. The **Manage Incident Reports** link is available under **Links** if you are granted permissions in Oracle PSIR. Use this link to access the administration and search pages.
8. Use the **Search Incidents** page to search for incident reports and update, close, or withdraw them. This is an Oracle Public Sector Incident Reporting page.
9. Use the **Search Incidents by Person** page to search for incident reports using person details. This is an Oracle Public Sector Incident Reporting page.
10. Use the **Search Incidents** page to search for incident reports narrowed down to a specific geographic location. This is an Oracle Public Sector Incident Reporting page.
11. Use the **Maintain Lookup Type Codes** page to modify lookup type code options for submitting an incident report. This is an Oracle Public Sector Incident Reporting administration page.
12. Use the **Maintain Responders and Jurisdiction Access** page to modify responder and jurisdiction access options for submitting an incident report. This is an Oracle Public Sector Incident Reporting administration page.
13. Use the **Maintain Global Lookup Type Codes** page to modify global lookup type code

options for submitting an incident report. This is an Oracle Public Sector Incident Reporting administration page.

14. Use the **Maintain Country and State Codes** page to modify country and state code options for submitting an incident report. This is an Oracle Public Sector Incident Reporting administration page.
15. The Oracle Business Process Workspace **My Tasks** page displays the incident reports an action officer, case worker, or case manager must take action on. This is an Oracle Business Process Management Workspace page.
16. For more information on how to work with tasks, such as reassigning a task, routing a task, or setting a vacation period, see "Working on Tasks in Process Workspace," in *Oracle Fusion Middleware User's Guide for Oracle Business Process Management*.
17. For more information on understanding, navigating, and setting your preferences in Oracle Business Process Workspace, see "Getting Started with Process Workspace," in *Oracle Fusion Middleware User's Guide for Oracle Business Process Management*.
18. You have completed the **Understanding Oracle Public Sector Incident Reporting Pages** topic.

### Starting Oracle Public Sector Incident Reporting

Oracle Public Sector Incident Reporting (PSIR) runs on Microsoft Internet Explorer 8.0 (or later), Chrome 11.x, or Mozilla Firefox 4.x (or later). You need a valid Oracle Business Process Management Workspace URL, user ID, and password to access Oracle PSIR. Contact your system administrator for the URL and your login credentials.

In this topic, you will see how to log into Oracle Business Process Management Workspace and access Oracle Public Sector Incident Reporting.

#### **Procedure: Starting Oracle Public Sector Incident Reporting**

1. To begin, enter **http://server name:port/bpm/workspace** in your web browser.  
  
Replace server name and port with the server name and port number you received from your administrator.  
  
The Oracle Business Process Workspace **Sign In** page opens.
2. Enter your username and password in the respective fields, then click **Login**.
3. You are now logged into Oracle Business Process Management Workspace.
4. Click the **Applications** link to access any Oracle Process Accelerator, implemented by your organization and that you have permissions to.
5. Use the **Report an Incident** link to access Oracle Public Sector Incident Reporting.
6. You have completed the **Starting Oracle Public Sector Incident Reporting** topic.

## Using Oracle Public Sector Incident Reporting

This section is intended for citizens and reporters who submit incident reports, and case workers and other personnel who manage and disposition incident reports.

Upon completion of this section, you will be able to:

- Submit an incident report.
- Review an incident report.
- Assess an incident report.
- Evaluate an incident report.
- Update an incident report.
- Assign a responder to an incident report.
- Associate related incident reports.
- Withdraw an incident report.
- Close an incident report.
- Search for incident reports using person details.
- Analyze incidents.
- View NIEM documents for an incident report.

### Submitting an Incident Report

Imagine you witness an incident and want to report it. You can use Oracle Public Sector Incident Reporting to submit an incident report. You can submit an incident one of the three following ways:

- PSIR UI
- Public UI
- Mobile phone

Your choice of UI depends on your role. As a reporter, you use the PSIR UI to submit incident reports. As a citizen, you use the public UI or your mobile phone.

In this topic, you will create and submit an incident report from the PSIR UI, the public UI, and a mobile phone.

#### ***Procedure: Submitting an Incident Report***

1. Begin by navigating to the **Enter Incident Report** page.  
Click the **Report an Incident** link.
2. Use the **Enter Incident Report** page to create and submit an incident report, if you are a reporter.

3. Use the **Incident** tab to enter incident details.
4. **Note:** All fields with an **Asterisk (\*)** are required.  
Click the **Type** list.
5. Click the **Arson** list item.
6. Selecting the **Arson** or **Traffic Accident** incident type displays a dynamic tab for additional incident details.
7. Click the **Severity** list.
8. Click the **Urgent** list item.
9. The date and time automatically populate when the **Enter Incident Report** page opens.
10. Click in the **Description** field.
11. Enter the desired information into the **Description** field. Enter "**Car on fire**".
12. Click the **Location Type** list.
13. Click the **Business Park** list item.
14. Click in the **Description** field.
15. Enter the desired information into the **Description** field. Enter "**Parking garage 3**".
16. Click in the **Street Address** field.
17. Enter the desired information into the **Street Address** field. Enter "**22 Main St**".

18. Click in the **City** field.
19. Enter the desired information into the **City** field. Enter "**Oakland**".
20. Click the **Country** list.
21. Click the **United States of America** list item.
22. Click the **State** list.
23. Click the **California** list item.
24. Click in the **Detailed Narration** field.
25. Enter the desired information into the **Detailed Narration** field. Enter "**Zoe Evans's car is on fire. No one is in the car.**".
26. Use the **Contact** tab to enter your contact information and the agency contact information if you notified someone.
27. Click the **People** tab.
28. Use the **People** tab to enter details for people involved in the incident. This could be an attacker, responder, suspect, victim, or witness.

The screenshot shows the 'Enter Incident Report' form with the following details:

- Description Section:**
  - \* Type: Arson
  - \* Severity: Urgent
  - \* Date and Time: 4/29/2013 2:38 PM
  - \* Description: Car on fire
- Location Section:**
  - Name of Business / Facility: (empty)
  - \* Location Type: Business Park
  - Description: Parking garage 3
  - \* Street Address: 22 Main St
  - \* City: Oakland
  - \* Country: United States of America
  - \* State: California
  - Zip Code: (empty)
- Detailed Narration:** Zoe Evans's car is on fire. No one is in the car.
- People Tab:** Selected, showing 'Add' and 'Delete' buttons and 'No data to display.'

29. Click the **Add** button.
30. Click the **Involvement Type** list.
31. Click the **Victim** list item.
32. Click in the **First Name** field.
33. Enter the desired information into the **First Name** field. Enter "**Zoe**".

34. Click in the **Last Name** field.
35. Enter the desired information into the **Last Name** field. Enter "**Evans**".
36. Click the **Vertical** scrollbar.
37. Click in the **Other Observations** field.
38. Enter the desired information into the **Other Observations** field. Enter "**Zoe's car is the one burning. Her number is 2095550125.**".
39. Click the **Is Injured ?** list.
40. Click the **No** list item.
41. Click the **Is Dead ?** list.
42. Click the **No** list item.
43. Click the **Arson** tab.
44. Use the **Arson** tab to enter details about the arson.

The screenshot shows a web form titled "Enter Incident Report". At the top right, there are "Actions" and "Submit" buttons. The form is divided into several sections:

- INCIDENT TYPE / INCIDENT**: Includes fields for Severity (set to "Urgent"), Date and Time (4/29/2013 2:38 PM), and Description (Car on fire).
- INCIDENT LOCATION / QUALITY**: Includes fields for Location Type (Business Park), Description (Parking garage 3), Street Address (22 Main St), City (Oakland), Country (United States of America), State (California), and Zip Code.
- Detailed Narration**: A text area containing the text "Zoe Evans's car is on fire. No one is in the car."
- Arson Tab**: This tab is selected and shows fields for Property Description, Estimated Damage (\$), Apparent Cause, Accelerant, No. Victims Injured, No. Victims Killed, and Responders on Site.

45. Click in the **No. Victims Injured** field.
  46. Enter the desired information into the **No. Victims Injured** field. Enter "**0**".
  47. Click the **Actions** menu.
  48. Use **Save** to save this incident report to edit later.
  49. Use the **Submit** button to save and submit the incident report.
- Click the **Submit** button.

50. Confirm that you want to submit the incident report.

Click the **Yes** button.

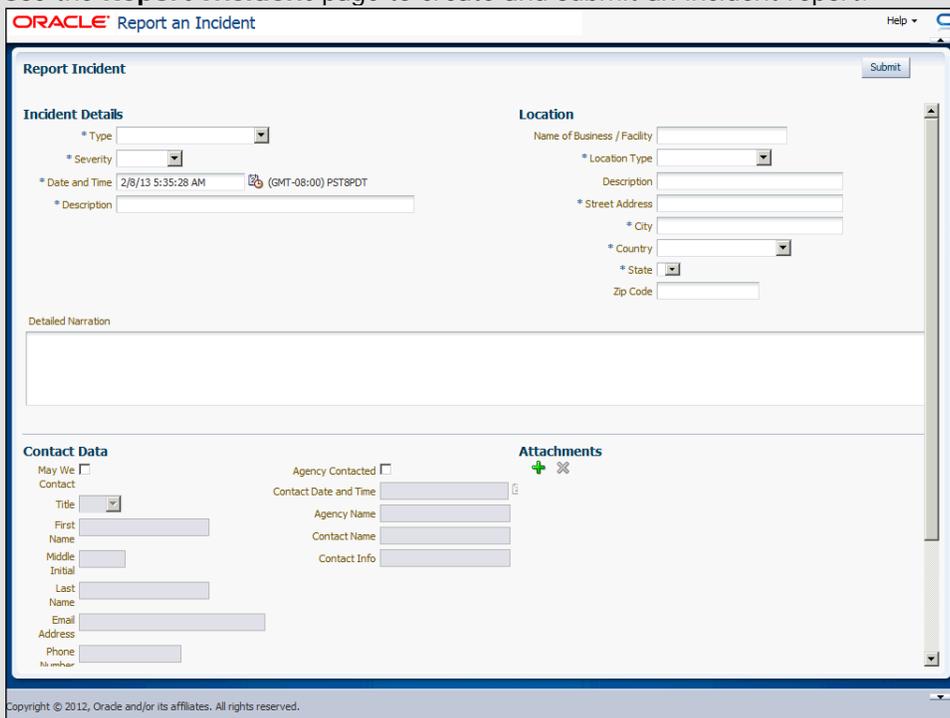
51. After you submit an incident report, it is routed to an action officer for review.

Next, submit an incident report from the public UI.

52. If you are a citizen, begin using the public UI by entering **http://server name:port/IncidentReportingPublicUI/faces/reportIncident.jspx** in your web browser.

Replace server name and port with the server name and port number you received from your administrator.

53. Use the **Report Incident** page to create and submit an incident report.



54. You complete the **Report Incident** page the same way as the **Enter Incident Report** page. In this example, the incident report has been completed for you.

55. Notice the **Report Incident** page does not have the tabs like the **Enter Incident Report** page. You do have the option to attach files.

56. Use the **Submit** button to save and submit the incident report.

Click the **Submit** button.

57. Click the **OK** button.

58. After you submit an incident report, it is routed to an action officer for review.

Next, submit an incident report from your mobile phone.

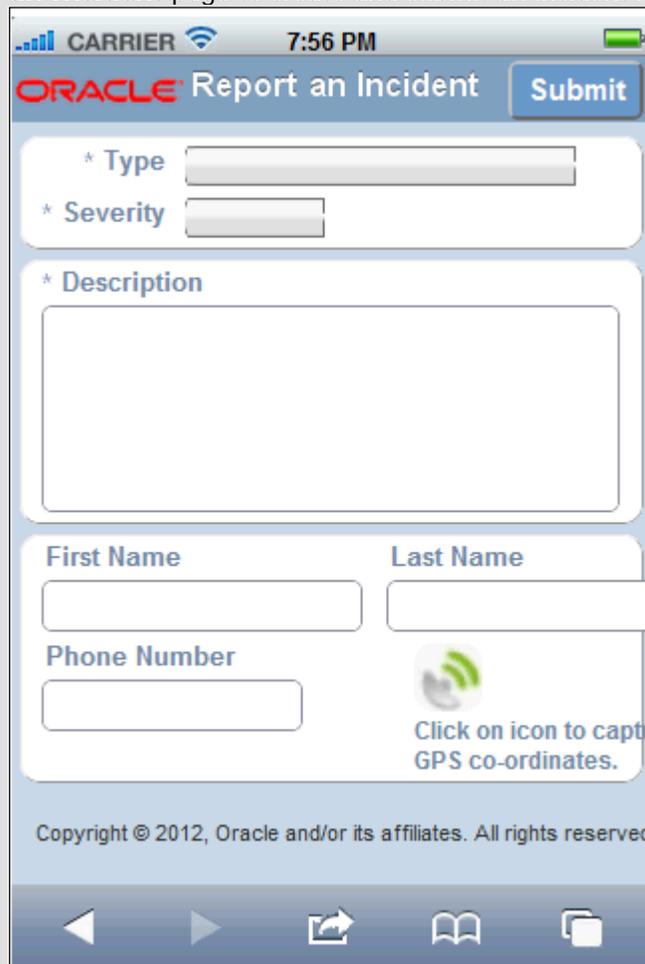
59. If you are a citizen, begin using the mobile UI by entering **http://server name:port/IncidentReportingMobileUI/faces/IncidentEntry.jspx** in your mobile

web browser.

Replace server name and port with the server name and port number you received from your administrator.

60. Click the **Report an Incident** link.

61. Use the **Report an Incident** page to create and submit an incident report.



The screenshot shows a mobile application interface for reporting an incident. At the top, the status bar displays 'CARRIER', signal strength, Wi-Fi, and the time '7:56 PM'. The app header features the 'ORACLE' logo, the text 'Report an Incident', and a 'Submit' button. Below the header, there are three required fields: '\* Type' (a dropdown menu), '\* Severity' (a dropdown menu), and '\* Description' (a large text area). Underneath these are fields for 'First Name' and 'Last Name', followed by a 'Phone Number' field. To the right of the phone number field is a green circular icon with a location pin, labeled 'Click on icon to capture GPS co-ordinates.'. At the bottom of the form area, there is a copyright notice: 'Copyright © 2012, Oracle and/or its affiliates. All rights reserved'. The bottom of the screen shows a standard Android navigation bar with back, home, and recent apps icons.

62. Click the **Type** list.

63. Click the **Arson** list item.

64. Click the **Severity** list.

65. Click the **Moderate** list item.

66. In this example, the rest of the information has been completed for you.

67. Click the **GPS Location** button.

68. The **GPS Button** allows your mobile phone to send your longitude and latitude location with the incident report.

When an action officer looks at the incident report, the incident location appears on their map.

Click the **OK** button.

69. Use the **Submit** button to submit the incident report.

Click the **Submit** button.

70. Click the **OK** button.

71. You have completed the **Submitting an Incident Report** topic.

## Reviewing an Incident Report

An action officer is assigned after an incident report is submitted. As an action officer, you can review the incident report and add local responders, then you must determine if:

- More information is required from the submitter.
- The incident report must be rejected.
- The incident report must be approved.

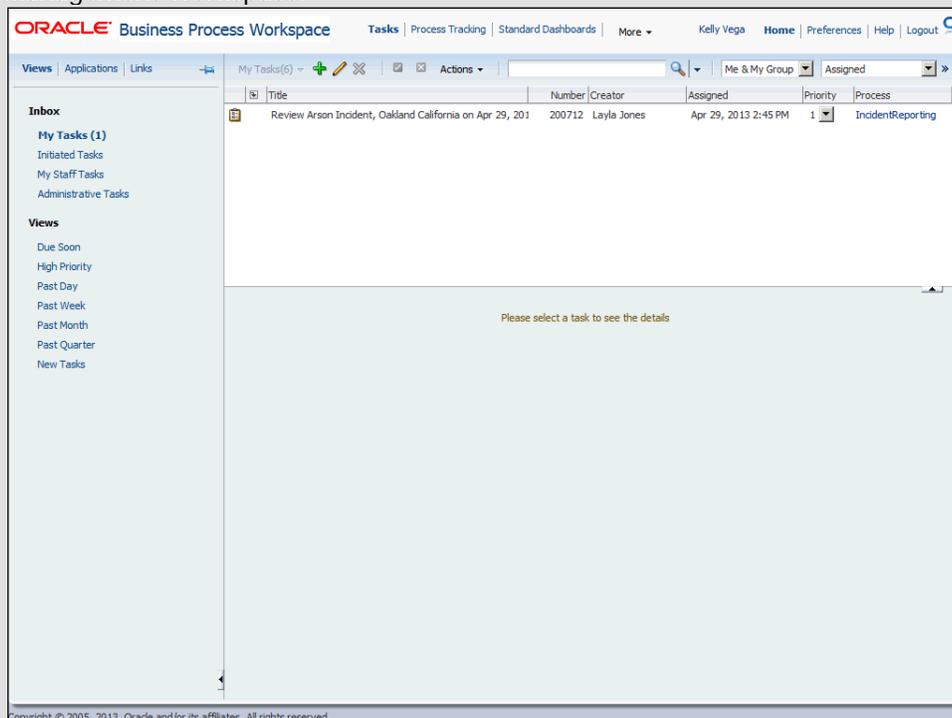
Once you approve the incident report it moves to the case worker.

In this topic, you will review, assign a responder, and approve an incident report.

### **Procedure: Reviewing an Incident Report**

1. Use the **My Tasks** page to view all incident reports on which you have to act.

The **My Tasks** page automatically opens after you log into Oracle Business Process Management Workspace.



2. Select the incident report task you want to review.

Click the task to open it in the **Task Details** section. Double-click the task to open in a

new window. In this example, you will double-click the task.

Double-click the **Task** object.

- Use the **Review Incident** page to review the incident report and add local responders.

- Use the **Claim** button to assign this task to yourself if multiple action officers are presented with this task.

- After reviewing the incident report, you determine you need to add that the fire department has been contacted and approve the report.

Click the **Responders** tab.

- Click the **Add** button.

- Click the **Vertical** scrollbar.

- The map pinpoints the incident location using an orange flag. A green flag represents responders nearest the incident.

- Once you assign the responder to the incident report, an email is sent to the contact informing them of the incident. The email information is automatically populated, but you can edit it.

- Click the **Fire Department** option.

- Click the **Assign** button.

- In some cases, incidents are related to each other by a system task using business rules, or by a case worker.

Click the **Related Incidents** tab.

13. In this case, no incidents have been automatically related to the current incident.
14. Use the **Request Details** button to ask the submitter for more information. You must enter a comment to request details.
15. Use the **Approve** button to approve this incident report.
 

Click the **Approve** button.
16. After you approve an incident report, it moves to the case worker for assessment.
17. You have completed the **Reviewing an Incident Report** topic.

## Assessing an Incident Report

As a case worker, you must assess an incident report to determine if a higher level response is required. You can assign responders whose jurisdiction maps to the case worker role. If a national or international responder is required, then you must escalate to a case manager. Besides escalating, you can approve an incident report, which enables you to extract it to a National Information Exchange Model (NIEM) compliant document, reject it, or claim it so no other case worker can update it.

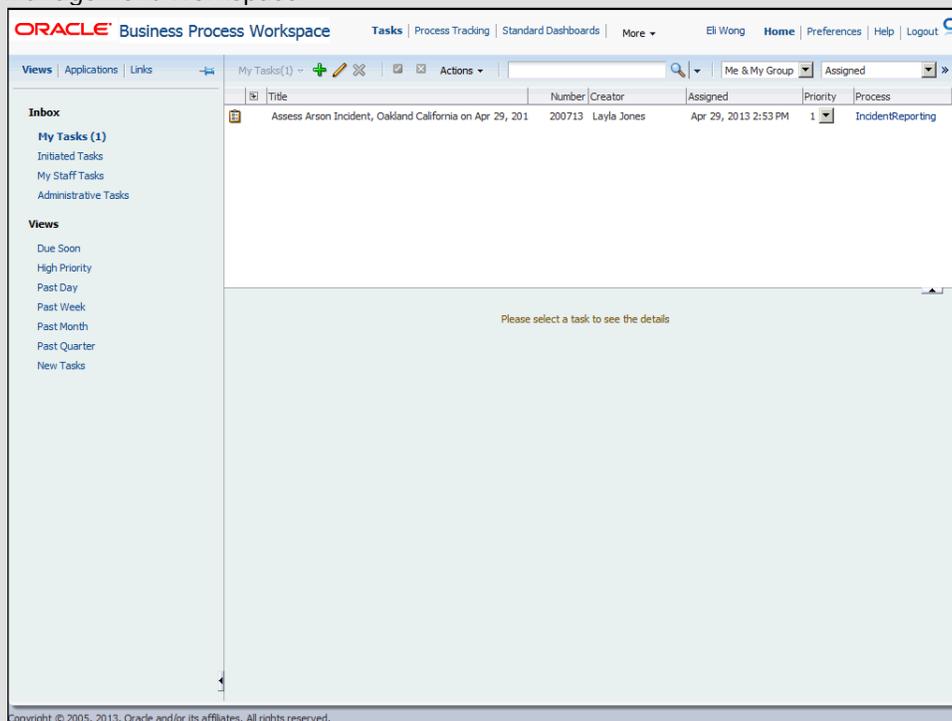
Another responsibility of a case worker is to assess the incident in relation to other incidents, and to determine if the current incident is a duplicate or part of a trend. Two tools support this responsibility, the Geographical Analysis, shown in the Analyzing Incident topic; and the ability to tie incidents together, shown in the Associating Related Incident Reports topic.

In this topic, you will assess an incident report and escalate it to the case manager.

### Procedure: Assessing an Incident Report

1. Use the **My Tasks** page to view all incident reports on which you have to act.

The **My Tasks** page automatically opens after you log into Oracle Business Process Management Workspace.



2. Select the incident report task you want to assess.

Click the task to open it in the **Task Details** section. Double-click the task to open in a new window. In this example, you will double-click the task.

Double-click the **Task** object.

3. Use the **Assess Incident** page to assess the incident report and add local responders.

4. Use the **Claim** button to assign this task to yourself if multiple case workers are presented with this task.
5. After assessing the incident report, you determine it must be escalated so additional security can be added. Comments are required to escalate an incident report.  
Click the **Comments** tab.
6. Click the **Create** button.
7. Enter the desired information into the **Comment** field. Enter "**We should set up additional security to monitor the parking garages.**".
8. Specify who should see the comments by selecting the appropriate option. This example uses the default **All process participants** option.
9. Click the **OK** button.
10. Use the **Approve** button to approve this incident report and optionally choose to extract it to a NIEM compliant document.
11. Use the **Escalate** button to escalate the incident report to a case manager. Comments are required.  
Click the **Escalate** button.

12. You have completed the **Assessing an Incident Report** topic.

## Evaluating an Incident Report

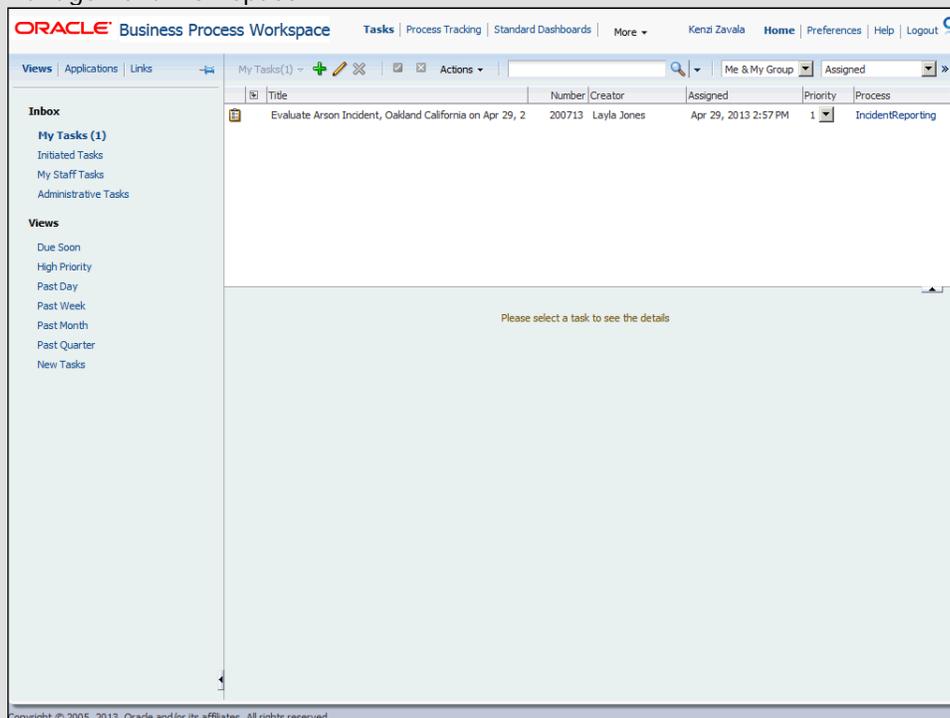
As a case manager, you are responsible for evaluating and assigning national and international responders to an incident report. You can assign responders whose jurisdiction maps to the case manager role. You can claim an incident report so no other case worker can update it. Once an incident report has been handled, you can approve it, which allows you to extract it to a National Information Exchange Model (NIEM) compliant document or reject it.

In this topic, you will approve and extract an incident report to a NIEM compliant document.

### Procedure: Evaluating an Incident Report

1. Use the **My Tasks** page to view all incident reports on which you have to act.

The **My Tasks** page automatically opens after you log into Oracle Business Process Management Workspace.



2. Select the incident report task you want to evaluate.

Click the task to open it in the **Task Details** section. Double-click the task to open in a new window. In this example, you will double-click the task.

Double-click the **Task** object.

3. Use the **Evaluate Incident** page to evaluate the incident report and add national and international responders.

4. Use the **Claim** button to assign this task to yourself if multiple case managers are presented with this task.
5. After evaluating the incident report you determine no additional responders are needed so you approve the incident report and extract it to a NIEM compliant document.  
Click the **Approve** button.
6. Click the **Yes** button.
7. You have completed the **Evaluating an Incident Report** topic.

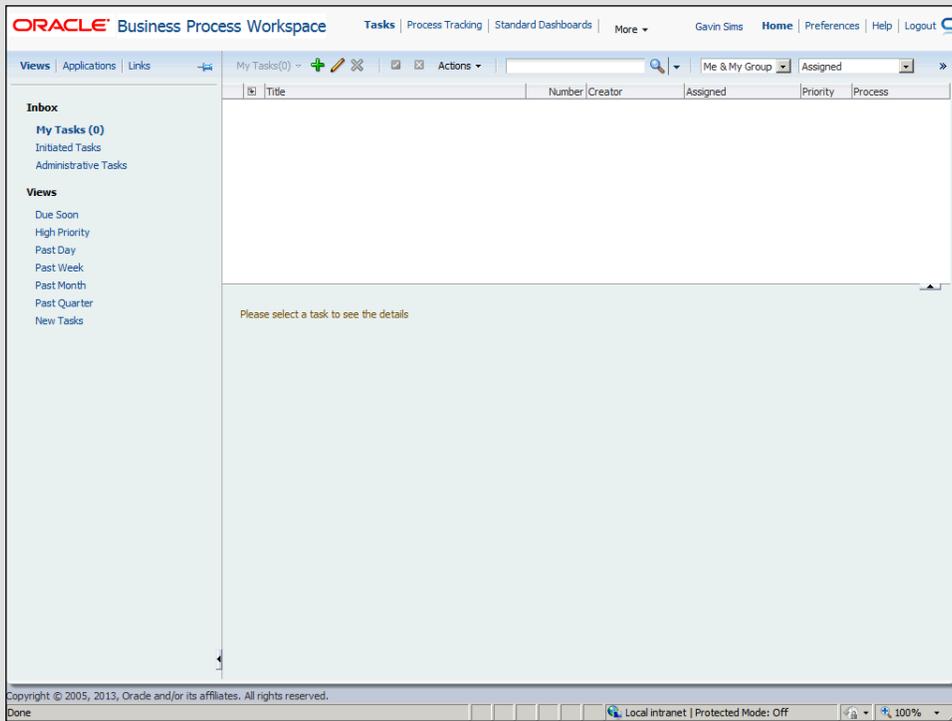
## Updating an Incident Report

You reported an arson incident. Now you want to update the arson details. Action officers, case workers, and case managers can also update an incident report.

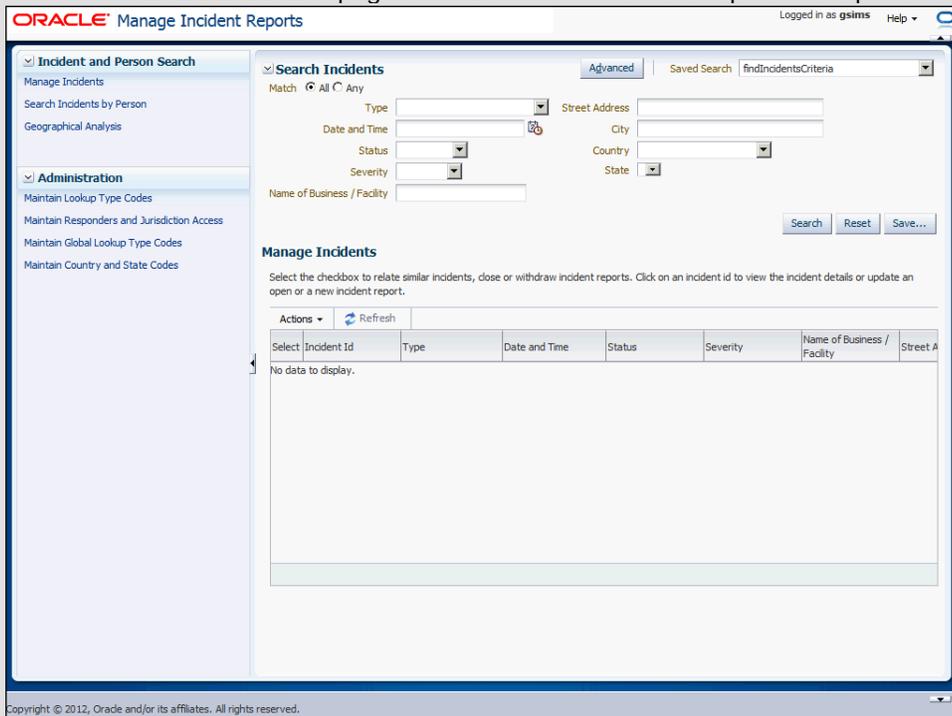
In this topic, you will update the arson details for an incident report.

### ***Procedure: Updating an Incident Report***

1. Begin by navigating to the **Search Incidents** page.  
Click the **Links** link.



2. Click the **Manage Incident Reports** link.
3. Use the **Search Incidents** page to search for an incident report and update it.



4. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, search criteria have been filled out for you.

Click the **Search** button.

5. The search lists incidents that match your criteria. Select the incident you want to

update.

Click the **Incident Id** link.

6. The incident report opens for editing.

Click the **Arson** tab.

7. Enter the arson details. In this example, the details have been completed for you.

8. Click the **Update** button.

9. You have completed the **Updating an Incident Report** topic.

## Assigning a Responder to an Incident Report

You need to assign a responder to an incident report. As an action officer, case worker, or case manager, you can assign responders to an incident report.

In this topic, you will assign a responder to an incident report.

### Procedure: Assigning a Responder to an Incident Report

1. Begin by navigating to the **Search Incidents** page.

Click the **Links** link.

2. Click the **Manage Incident Reports** link.

3. Use the **Search Incidents** page to search for incident reports.

The screenshot shows the Oracle Manage Incident Reports application interface. The top navigation bar includes the Oracle logo, the title 'Manage Incident Reports', and user information 'Logged in as kzavala' with a 'Help' dropdown. A left sidebar contains navigation links: 'Incident and Person Search', 'Manage Incidents', 'Search Incidents by Person', and 'Geographical Analysis'. The main content area is titled 'Search Incidents' and features an 'Advanced' search mode. It includes a 'Match' dropdown set to 'All', and several search criteria fields: 'Type', 'Date and Time', 'Status', 'Severity', 'Name of Business / Facility', 'Street Address', 'City', 'Country', and 'State'. Below the search fields are 'Search', 'Reset', and 'Save...' buttons. A section titled 'Manage Incidents' contains instructions and an 'Actions' dropdown with a 'Refresh' button. Below this is a table with columns: 'Select', 'Incident Id', 'Type', 'Date and Time', 'Status', 'Severity', 'Name of Business / Facility', and 'Street A'. The table currently displays 'No data to display.' and has a scrollbar at the bottom.

4. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, search criteria have been fill out for you.

Click the **Search** button.

- The search lists incidents that match your criteria. Select the incident you want to assign a responder to.

Click the **Incident Id** link.

- Click the **Responders** tab.

- Click the **Add** button.

- Click the **Vertical** scrollbar.

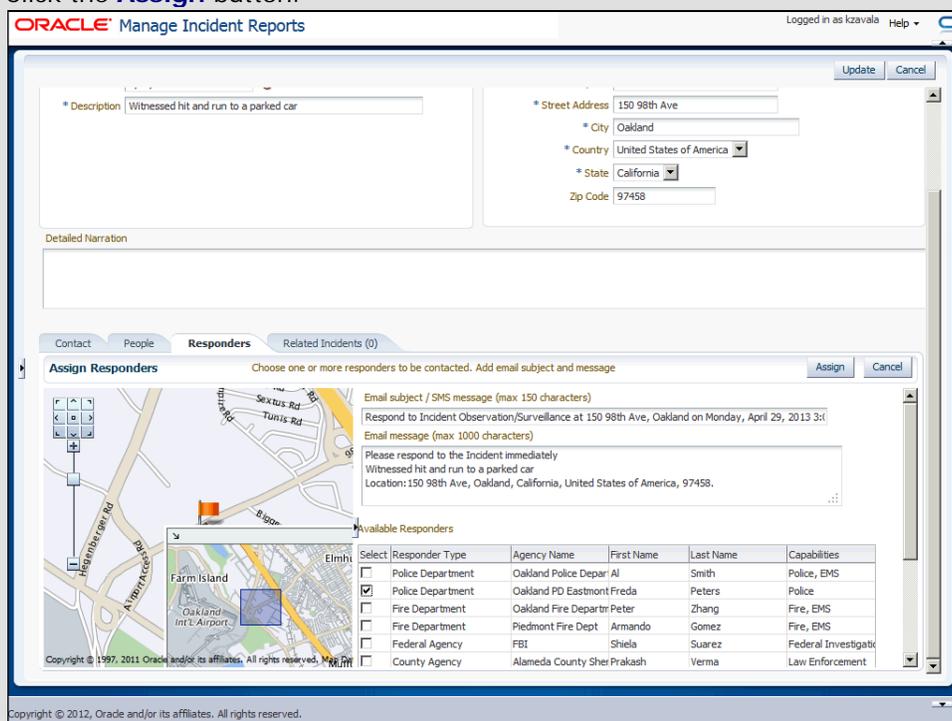
- Click the **Collapse Pane** button.

- The map pinpoints the incident location using an orange flag. A green flag represents responders nearest to the incident location.

- Once you assign the responder to the incident report, an email is sent to the contact, informing them of the incident. The email information is automatically populated but you can edit it.

- Click the **Police Department** option.

- Click the **Assign** button.



- The Police Department is now an assigned responder. You can click **Add** to continue adding more responders, if needed.

- Click the **Update** button.

- Click the **Ok** button.

- You have completed the **Assigning a Responder to an Incident Report** topic.

## Associating Related Incident Reports

Several incident reports for graffiti at schools have been reported. As an action officer, case worker, or case manager, you can associate related incident reports.

Two ways exist to relate incident reports. The first method is to use the **Related Incidents** tab in an incident report. The second method is to use the **Actions** menu on the **Manage Incidents** page.

In this topic, you will associate related incident reports, using both methods.

### Procedure: Associating Related Incident Reports

1. Begin by navigating to the **Search Incidents** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Use the **Search Incidents** page to search for incident reports.

The screenshot shows the Oracle Manage Incident Reports interface. The top navigation bar includes the Oracle logo, the page title "Manage Incident Reports", and the user "gsims". The main content area is divided into a left sidebar and a main panel. The sidebar contains "Incident and Person Search", "Manage Incidents", "Search Incidents by Person", and "Geographical Analysis". The main panel has a "Search Incidents" section with a "Match" dropdown set to "All", and several search criteria fields: "Type", "Date and Time", "Status", "Severity", "Name of Business / Facility", "Street Address", "City", "Country", and "State". Below these fields are "Search", "Reset", and "Save..." buttons. A "Manage Incidents" section follows, with a "Select" checkbox and a "Refresh" button. Below this is a table with columns: "Select", "Incident Id", "Type", "Date and Time", "Status", "Severity", "Name of Business / Facility", and "Street A". The table currently displays "No data to display."

4. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, search criteria have been filled out for you.  
Click the **Search** button.
5. The search lists incidents that match your criteria. Select the incident you want to associate related incidents to.  
Click the **Incident Id** link.
6. Click the **Related Incidents (0)** tab.
7. Click the **Add** button.

8. In this example, search criteria have been filled out for you.  
Click the **Search** button.
9. Select the incidents you want to associate to the current incident. In this example, three incidents have been selected for you.  
Click the **Relate** button.
10. Click the **OK** button.
11. Click the **Close** button.
12. Click the **Update** button.
13. Alternatively, you can relate incidents from the **Manage Incidents** page by using the **Actions** menu to relate incidents directly.  
First, select the incidents you want to relate.  
Click the **Select** option.
14. Click the **Select** option.
15. Click the **Select** option.
16. Click the **Actions** menu.
17. The **Relate Incidents** option is available when more than one incident report is selected.  
Click the **Relate Incidents** menu.
18. A dialog box confirms that the incidents have been related.  
Click the **OK** button.
19. You have completed the **Associating Related Incident Reports** topic.

## Withdrawing an Incident Report

You want to withdraw a false incident report. As an action officer, case worker, or case manager, you can withdraw an incident report.

In this topic, you will withdraw an incident report.

### ***Procedure: Withdrawing an Incident Report***

1. Begin by navigating to the **Search Incidents** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Use the **Search Incidents** page to search for an incident report and withdraw it.

4. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, the search criteria have been filled out for you.

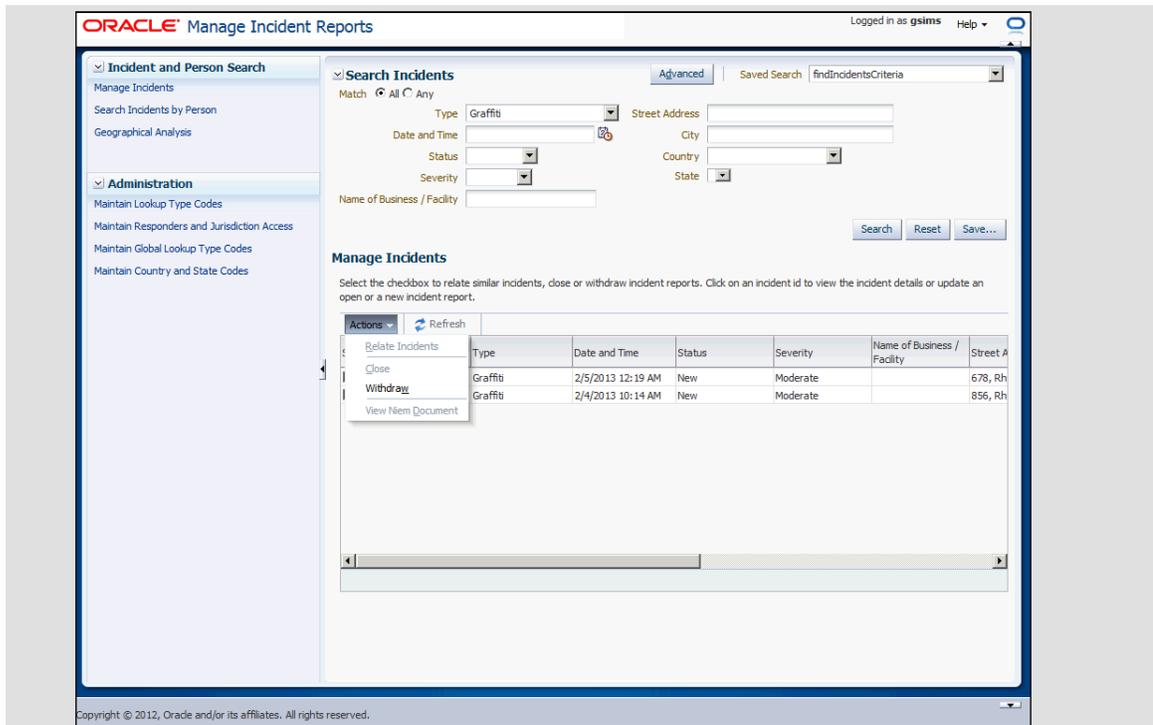
Click the **Search** button.

5. The search lists incidents that match the search criteria. Select the incident report you want to withdraw.

Click the **Select** option.

6. Click the **Actions** menu.

7. Click the **Withdraw** list item.



8. Click the **OK** button.
9. The incident is withdrawn and the status is changed to **Withdrawn**.
10. You have completed the **Withdrawing an Incident Report** topic.

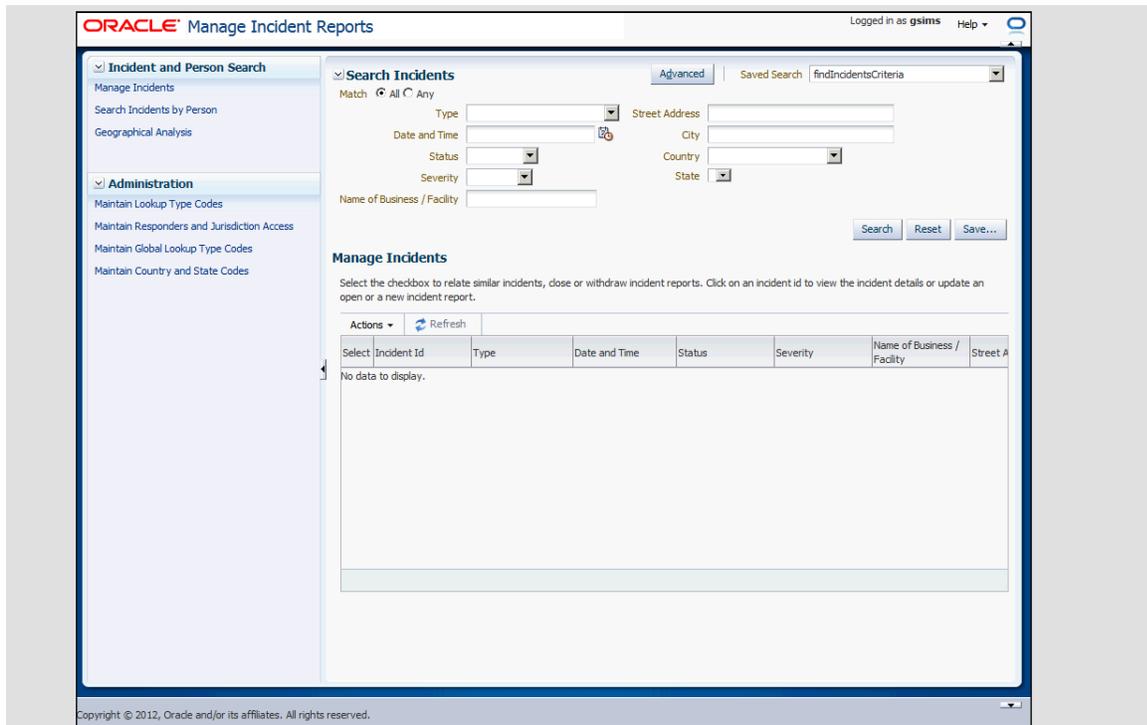
## Closing an Incident Report

A case manager can close an incident report after it has been fully investigated.

In this topic, you will close an incident report.

### ***Procedure: Closing an Incident Report***

1. Begin by navigating to the **Search Incidents** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Use the **Search Incidents** page to search for an incident report and close it.



4. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, search criteria have been filled out for you.

Click the **Search** button.

5. The search lists incidents that match your criteria. Select the incident report you want to close.

Click the **Select** option.

6. Click the **Actions** menu.

7. Click the **Close** list item.

8. Click the **OK** button.

9. The incident is closed and the status is changed to **Closed**.

10. You have completed the **Closing an Incident Report** topic.

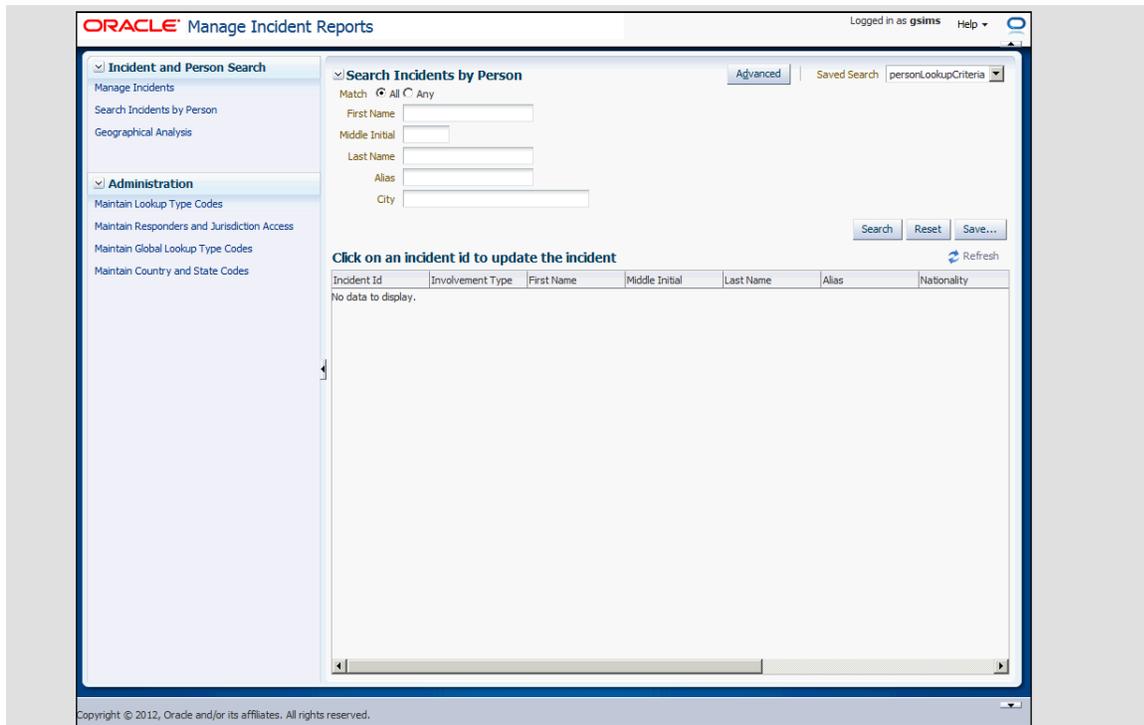
## Searching Incidents by Person

You don't remember the details of an incident report to perform a standard search, but you remember the suspect's name. You can use the **Search Incident by Person** page to search using person details.

In this topic, you will search for an incident report using person details.

### **Procedure: Searching Incidents by Person**

1. Begin by navigating to the **Search Incident by Person** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Search Incidents by Person** link.
4. Use the **Search Incidents by Person** page to search for incident reports using person details.



5. You can specify search criteria or click **Search** without criteria to list all incident reports. In this example, search criteria have been filled out for you.

Click the **Search** button.

6. The search lists incidents that match your criteria.
7. You have completed the **Search Incidents by Person** topic.

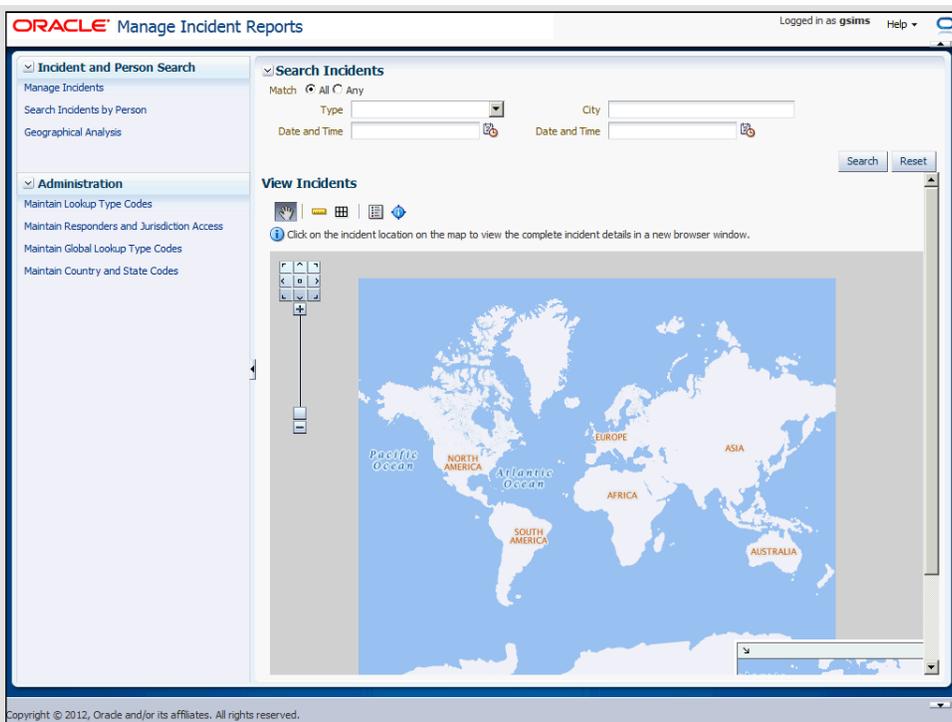
## Analyzing Incidents

You need to analyze several incidents within a specific geographical location. You can determine the priority, distance, area, and longitude and latitude of these incidents.

In this topic you will, analyze incidents based on their geographical location.

### **Procedure: Analyzing Incidents**

1. Begin by navigating to the **Search Incidents** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Geographical Analysis** link.
4. Use the **Search Incidents** page to search for incident reports within a particular geographic location.



5. In this example, search criteria have been filled out for you.

Click the **Search** button.

6. The **Pan** button enables you to navigate across the map.

7. Selecting a flag allows you to view the details of the incident.

Click the **Orange Flag**.

8. Use the **View Incident Details** page to view the details for the selected incident report. After viewing the report, return to the **Search Incidents** page.

To do this in real time, you must press **[Alt+Tab]** on your keyboard to return to the previous window. However, to proceed with the tutorial, press **Enter**.

9. The **Distance** button helps you see the total distance between two or more incident flags when you connect them.

Click the **Distance** button.

10. Select the first incident.

Click the **Blue Flag**.

11. Select the second incident.

Click the **Orange Flag**.

12. A line automatically connects the two incident flags as shown here.

13. Click the **Vertical** scrollbar.

14. The distance between the two incidents is indicated at the bottom left corner of the map.

15. Click the **Vertical** scrollbar.
16. The **Area** button enables you to view the total area between two or more geographical locations.  
  
Click the **Area** button.
17. Select the first incident.  
  
Click the **Blue Flag**.
18. Select the second incident.  
  
Click the **Orange Flag**.
19. Select a third incident.  
  
Click the **Orange Flag**.
20. Click the **Vertical** scrollbar.
21. The total area between these incidents is indicated at the bottom left corner of the map.
22. Click the **Vertical** scrollbar.
23. The **Legend** button enables you to see how the incidents are color-coded on the map.  
  
Click the **Legend** button.
24. A dialog box indicating the color codes for the incident priorities Low, Moderate, and Urgent opens.
25. Click the **Close** button.
26. The **Information** button provides the latitude and longitude of a location as your mouse hovers over it.  
  
Click the **Information** button.
27. Click the **Vertical** scrollbar.
28. The latitude and longitude of the incident report's location are visible at the bottom left corner of the map. You can get the latitude and longitude of any location by positioning your mouse over the desired point.
29. You have completed the **Analyzing Incidents** topic.

## Viewing NIEM Documents for an Incident Report

As a case manager or case worker you can view the NIEM document for an incident report.

In this topic, you will view an NIEM document.

### ***Procedure: Viewing NIEM Documents for an Incident Report***

1. Begin by navigating to the **Search Incidents** page.  
  
Click the **Links** link.

2. Click the **Manage Incident Reports** link.
3. Use the **Search Incidents** page to search for an incident report and view its NIEM Document, if generated. You can only view NIEM Documents for incidents with the Closed or Approved status.

4. In this example, search criteria have been filled out for you.  
Click the **Search** button.
5. Click the **Select** option.
6. Click the **Actions** menu.
7. Click the **View Niem Document** list item.
8. The NIEM Document opens in a new window. It is a plain XML file. After viewing the document, return to the **Search Incidents** page.

To do this in real time, you must press **[Alt+Tab]** on your keyboard to return to the previous window. However, to proceed with the tutorial, press **Enter**.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<IncidentReport xsi:schemaLocation="http://www.it.ojp.gov/jxdm/doc/incident/1.1/document">
- <DocumentDescriptiveMetadata>
  - <DocumentID>
    <ID>PSIR000089</ID>
  </DocumentID>
  <DocumentDescriptionText>NIEM Compliant document of the Incident Report </DocumentDescriptionText>
  - <DocumentAuthor.Organization>
    <OrganizationName>Oracle Corporation</OrganizationName>
    <OrganizationTypeText>Public Sector</OrganizationTypeText>
  </DocumentAuthor.Organization>
</DocumentDescriptiveMetadata>
- <ServiceCall>
  - <ActivityID>
    <ID>PSIR000089</ID>
    <ActivityDescriptionText>Incident of Graffiti reported</ActivityDescriptionText>
    <ActivityDate>2013-02-10</ActivityDate>
    <ActivityTime>20:08:00</ActivityTime>
  - <ServiceCallOriginator>
    - <PersonName>
      <PersonPrefixName>
      <PersonGivenName>
      <PersonMiddleName>
      <PersonSurName>
    </PersonName>
    </ServiceCallOriginator>
  </ActivityID>
</ServiceCall>
- <IncidentReportIncident>
  - <ActivityID>
    <ID>PSIR000089</ID>
  </ActivityID>
  <ActivityDescriptionText>Incident of Graffiti reported</ActivityDescriptionText>
  <ActivityDate>2013-02-10</ActivityDate>
  <ActivityTime>20:08:00</ActivityTime>
```

9. You have completed the **Viewing NIEM Documents for an Incident Report** topic.

## Administering Oracle Public Sector Incident Reporting

This section is intended for administrators who maintain Oracle Public Sector Incident Reporting (PSIR).

As an administrator, you can install Oracle PSIR and begin using the process accelerator as delivered. You can also modify Oracle PSIR to fit the needs of your organization. This section covers the data elements you can modify.

Upon completion of this section, you will be able to:

- Maintain Oracle Public Sector Incident Reporting drop-down lists.
- Describe the Oracle Public Sector Incident Reporting business rules.
- Describe the Oracle Public Sector Incident Reporting reports.

## Maintaining Oracle Public Sector Incident Reporting Drop-down Lists

This section is intended for administrators who maintain Oracle Public Sector Incident Reporting (PSIR).

Oracle Public Sector Incident Reporting ships with seeded data for drop-down lists. This section covers the drop-down lists you can modify.

Upon completion of this section, you will be able to:

- Maintain lookup type codes.
- Maintain responders.
- Maintain jurisdiction access.
- Maintain global lookup type codes.
- Maintain country codes.
- Maintain state codes.

### ***Maintaining Lookup Type Codes***

Lookup type codes specify values used in incident reports. Oracle Public Sector Incident Reporting ships with seeded values for lookup type codes. The seeded values are:

Incident Type

- Arson
- Burglary
- Assault
- Car Jacking
- Cyber Attack
- Drug Related Activity
- Emotionally Disturbed Person
- Fraud
- Graffiti
- Graffiti, Political

- Homicide
- Materials Acquisition
- Observation/Surveillance
- Public Health Threat
- Traffic Accident
- Weapons Discovery

Incident Status

- New
- Open
- Withdrawn
- Closed
- Invalid

Incident Severity

- Trivial
- Moderate
- Urgent

Incident Location Type

- Business
- Business Park
- Government Building
- Highway
- Hospital
- Industry
- Mall
- Open Area
- Park
- Private Home
- School
- Street

Person Involvement Type

- Witness
- Suspect
- Victim
- Attacker

- Responder

#### Responder Jurisdiction Type

- City
- State
- County
- Federal
- International

#### Responder Type

- Animal Control
- Emergency Medical Services
- Environmental Protection
- Federal Agency
- Fire Department
- International Agency
- Police Department
- Social Services
- State Agency
- State Police
- County Agency

#### Vehicle Type

- Truck
- Car
- Sports Utility Vehicle (SUV)
- Pickup Truck
- Motor Cycle

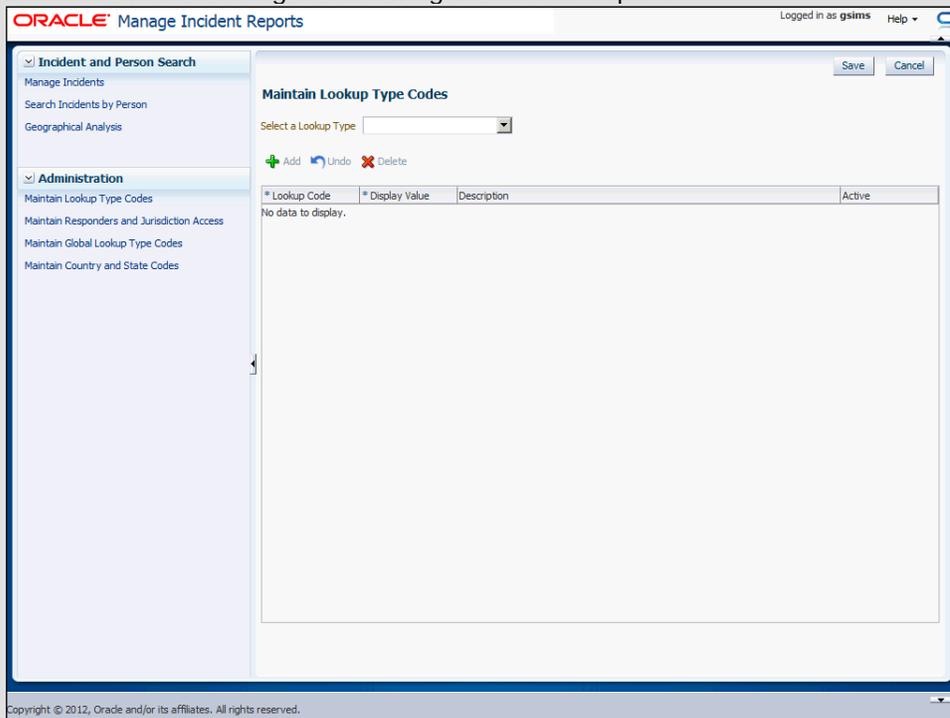
You can add additional lookup type codes to meet your organization's needs.

In this topic, you will modify lookup type code options.

#### ***Procedure: Maintaining Lookup Type Codes***

1. Begin by navigating to the **Maintain Lookup Type Codes** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Lookup Type Codes** link.

- Use the **Maintain Lookup Type Codes** page to modify the lookup type codes made available when creating or reviewing an incident report.



- Click the **Select a Lookup Type** list.
- These are the lookup types shipped with Oracle PSIR. You modify all lookup types using the same steps. In this topic, you will modify the **Incident Location Type**.

Click the **Incident Location Type** list item.

- First, add a lookup type code.

Click the **Add** button.

- Lookup Codes** are unique keys in the data tables and built into the logic of Oracle PSIR.

Click in the **Lookup Code** field.

- A **Lookup Code** can be upper or lower case.

Enter the desired information into the **Lookup Code** field. Enter **"WATER"**.

- Next, specify a short display value. Display values appear when an incident report is created or reviewed.

Click in the **Display Value** field.

- Enter the desired information into the **Display Value** field. Enter **"Waterway"**.

- Use the **Description** field to add an optional description.

Click in the **Description** field.

- Enter the desired information into the **Description** field. Enter **"The lookup code entry for incident location type Water."**

14. Saving the lookup type code makes it available when you create incident reports.  
Click the **Save** button.
15. The lookup type code **Waterway** is now added.
16. Next, modify the **Waterway** lookup type code by editing the description.  
Click in the **Description** field.
17. Enter the desired information into the **Description** field. Enter "**The lookup code entry for incident location type Waterway.**".
18. You can reverse any modifications to a single selected row using the **Undo** button. To save the modification, you would click **Save** instead.  
Click the **Save** button.
19. There are two types of delete, a hard delete and soft delete.  
A hard delete removes the lookup type code from the database table, provided it is not used in an incident report.  
First, perform a hard delete on the code **Waterway**.  
Click an entry in the row.
20. Click the **Delete** button.
21. Confirm that you want to delete the **Waterway** lookup type code.  
Click the **Yes** button.
22. Click the **Save** button.
23. The lookup type code **Waterway** is now deleted.
24. A soft delete inactivates a lookup type code already used in incident reports. Inactivated codes are not displayed as options for creating or reviewing incident reports.  
Next, perform a soft delete on the **Open Area** code.  
Click the **Active** option.
25. Click the **Save** button.
26. The lookup type code **Open Area** is now inactive.
27. You have completed the **Maintaining Lookup Type Codes** topic.

### ***Maintaining Responders***

Responders are public agencies assigned to respond to an incident when immediate action is necessary. Oracle Public Sector Incident Reporting ships with seeded values for responders. The seeded values are:

- Animal Control
- Emergency Medical Services

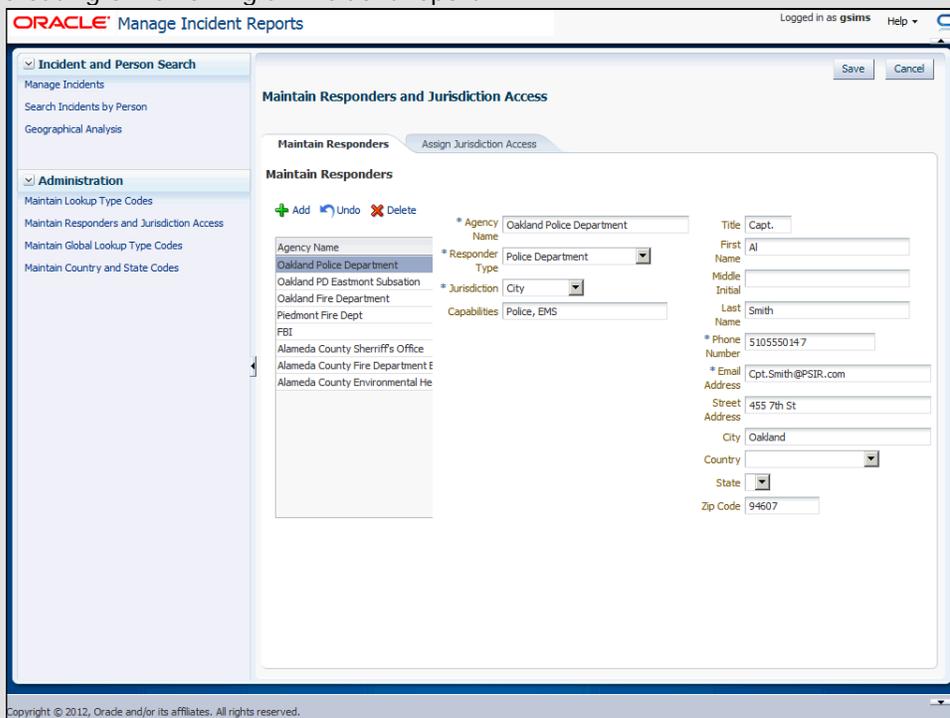
- Environmental Protection
- Federal Agency
- Fire Department
- International Agency
- Police Department
- Social Services
- State Agency
- State Police
- County Agency

You can add additional responders to meet your organization's needs.

In this topic, you will modify the responder options.

### Procedure: Maintaining Responders

1. Begin by navigating to the **Maintain Responders and Jurisdiction Access** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Responders and Jurisdiction Access** link.
4. Use the **Maintain Responders and Jurisdiction Access** page to modify the responders and jurisdiction access options made available when creating or reviewing an incident report.
5. Use the **Maintain Responders** tab to modify the responders made available when creating or reviewing an incident report.



6. First, add a responder.  
Click the **Add** button.
7. Click in the **Agency Name** field.
8. Enter the desired information into the **Agency Name** field. Enter "**New York Police Department**".
9. **Note:** All fields with an Asterisk (\*) are required.  
Click the **Responder Type** list.
10. **Note:** The responder types you see here are maintained on the **Maintain Lookup Type Codes** page.  
Click the **Police Department** list item.
11. Click the **Jurisdiction** list.
12. Click the **State** list item.
13. Click in the **Capabilities** field.
14. Enter the desired information into the **Capabilities** field. Enter "**Police**".
15. Next, enter the contact information for the responder.  
Click in the **Title** field.
16. Enter the desired information into the **Title** field. Enter "**Ms.**".
17. Click in the **First Name** field.
18. Enter the desired information into the **First Name** field. Enter "**Lucy**".
19. Click in the **Last Name** field.
20. Enter the desired information into the **Last Name** field. Enter "**Hattori**".
21. In this example, the remaining contact information fields are completed for you.
22. Saving the responder makes it available when you create or review incident reports.  
Click the **Save** button.
23. The responder **New York Police Department** is now added.
24. Next, modify the responder **New York Police Department** by updating the City field.  
Click in the **City** field.
25. Enter the desired information into the **City** field. Enter "**Rochester**".
26. All modifications must be saved.  
Click the **Save** button.

27. The contact information details for the responder are now modified.
28. Next, delete a responder from the responder list. Ensure that the responder to be deleted is selected from the list. Here, the responder **New York Police Department** is selected.  
  
Click the **Delete** button.
29. Confirm the deletion of the responder.  
  
Click the **Yes** button.
30. The responder **New York Police Department** is now removed.
31. You can reverse any modifications to a single selected row using the **Undo** button. To save the modification, you would click **Save** instead.
32. Saving ensures that the removed responder is no longer available to create or review incident reports.  
  
Click the **Save** button.
33. You have completed the **Maintaining Responders** topic.

### ***Maintaining Jurisdiction Access***

As access to an incident moves from action officer, to case worker, to case manager, access to responders increases, as controlled by the jurisdiction. Jurisdictions are assigned to roles to control which responders a role can access when assigning responders to an incident. (Jurisdictions are assigned to responders on the Maintain Responders tab.)

Oracle Public Sector Incident Reporting ships with seeded values for jurisdiction access. The seeded values are:

- City
- State
- County
- Federal
- International

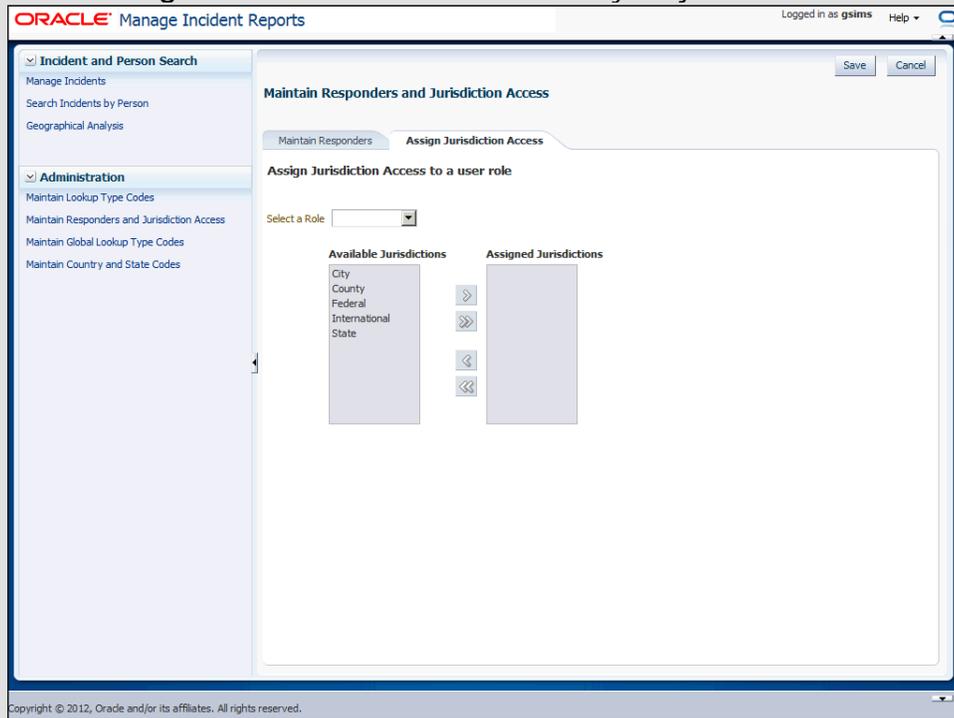
You can modify a role's jurisdiction access to meet your organization's needs.

In this topic, you will modify a role's jurisdiction access.

### ***Procedure: Maintaining Jurisdiction Access***

1. Begin by navigating to the **Maintain Responders and Jurisdiction Access** page.  
  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Responders and Jurisdiction Access** link.
4. Use the **Maintain Responders and Jurisdiction Access** page to modify the responders and jurisdiction access options made available when creating or reviewing an incident report.

5. Click the **Assign Jurisdiction Access** tab.
6. Use the **Assign Jurisdiction Access** tab to modify the jurisdiction for a role.



7. First, select the role you will assign jurisdiction access to.  
Click the **Select a Role** list.
8. In this example, we are going to assign the **International** jurisdiction to a Case Worker.  
Click the **Case Worker** list item.
9. Click the **International** list item.
10. Click the **Move selected items to other list** button.
11. The jurisdiction access **International** is now added.
12. Saving assigns the jurisdiction access to the selected role.  
Click the **Save** button.
13. Next, delete a specific jurisdiction access assigned to a role.  
Click the **Select a Role** list.
14. In this example, you will revoke the **STATE** jurisdiction from the Action Officer role.  
Click the **Action Officer** list item.
15. Select the jurisdiction that you want to delete for the specified role.  
Click the **State** list item.
16. Click the **Remove selected items from list** button.

17. Saving this change ensures that the **STATE** jurisdiction is no longer available for the Action Officer role.

Click the **Save** button.

18. You have completed the **Maintaining Jurisdiction Access** topic.

### ***Maintaining Global Lookup Type Codes***

Global lookup type codes specify global values used in incident reports. Oracle Public Sector Incident Reporting ships with seeded values for global lookup type codes. The seeded values are:

#### Yes/No Values

- Yes
- No

#### Person Title

- Mr.
- Mrs.
- Miss

#### Priority

- High
- Medium
- Low

#### Gender

- Male
- Female
- Unknown

#### Marital Status

- Married
- Unmarried
- Divorced
- Other

#### Nationality

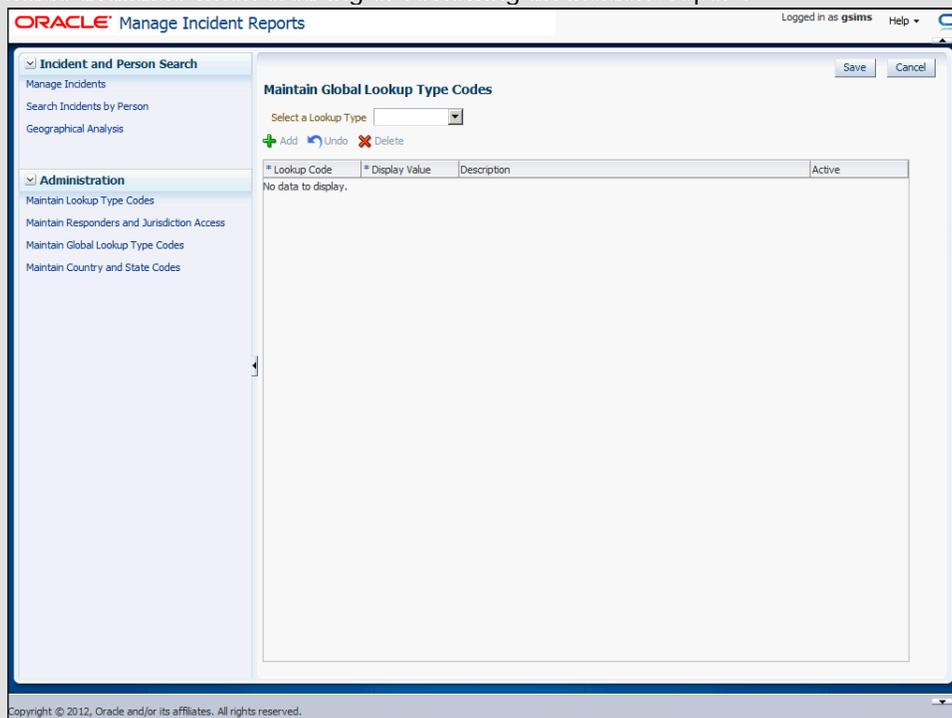
- Indian
- American

You can add additional global lookup type codes to meet your organization's needs.

In this topic, you will modify global lookup type code options.

### Procedure: Maintaining Global Lookup Type Codes

1. Begin by navigating to the **Maintain Global Lookup Type Codes** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Global Lookup Type Codes** link.
4. Use the **Maintain Global Lookup Type Codes** page to modify the lookup type codes made available when creating or reviewing an incident report.



5. Click the **Select a Look up Type** list.
6. These are the global lookup types shipped with Oracle PSIR. You modify all global lookup types using the same steps. In this topic, you will modify the **Marital Status**.  
Click the **Marital Status** list item.
7. First, add a global lookup type code.  
Click the **Add** button.
8. **Lookup Codes** are unique keys in the data tables and built into the logic of Oracle PSIR.  
Click in the **Lookup Code** field.
9. A **Lookup Code** can be upper or lower case.  
Enter the desired information into the **Lookup Code** field. Enter "**WID**".
10. Next, specify a short display value. Display values appear when an incident report is

created or reviewed.

Click in the **Display Value** field.

11. Enter the desired information into the **Display Value** field. Enter "**Widowed**".

12. Use the **Description** field to add an optional description.

Click in the **Description** field.

13. Enter the desired information into the **Description** field. Enter "**Spouse deceased**".

14. Saving the global lookup type code makes it available when you create incident reports.

Click the **Save** button.

15. The global lookup type code **Widowed** is now added.

16. Next, modify the **Widowed** global lookup type code by editing the description.

Click in the **Description** field.

17. Enter the desired information into the field. Enter "**Spouse deceased and not remarried.**".

18. You can reverse any modifications to a single selected row using the **Undo** button. To save the modification, you would click **Save** instead.

Click the **Undo** button.

19. There are two types of delete, a hard delete and soft delete.

A hard delete removes the global lookup type code from the database table, provided it is not used in an incident report.

First, perform a hard delete on the code **Widowed**.

Click an entry in the row.

20. Click the **Delete** button.

21. Confirm that you want to delete the **Widowed** global lookup type code.

Click the **Yes** button.

22. Click the **Save** button.

23. The global lookup type code **Widowed** is now deleted.

24. A soft delete inactivates a global lookup type code already used in incident reports. Inactivated codes are not displayed as options for creating or reviewing incident reports.

Next, perform a soft delete on the **Other** code.

Click the **Active** option.

25. Click the **Save** button.

26. The global lookup type code **Other** is now inactive.

27. You have completed the **Maintaining Global Lookup Type Codes** topic.

### ***Maintaining Country Codes***

Country codes enable a reporter or citizen to specify the country where the incident occurred when creating an incident report. Oracle Public Sector Incident Reporting ships with seeded values for country codes. The seeded values are:

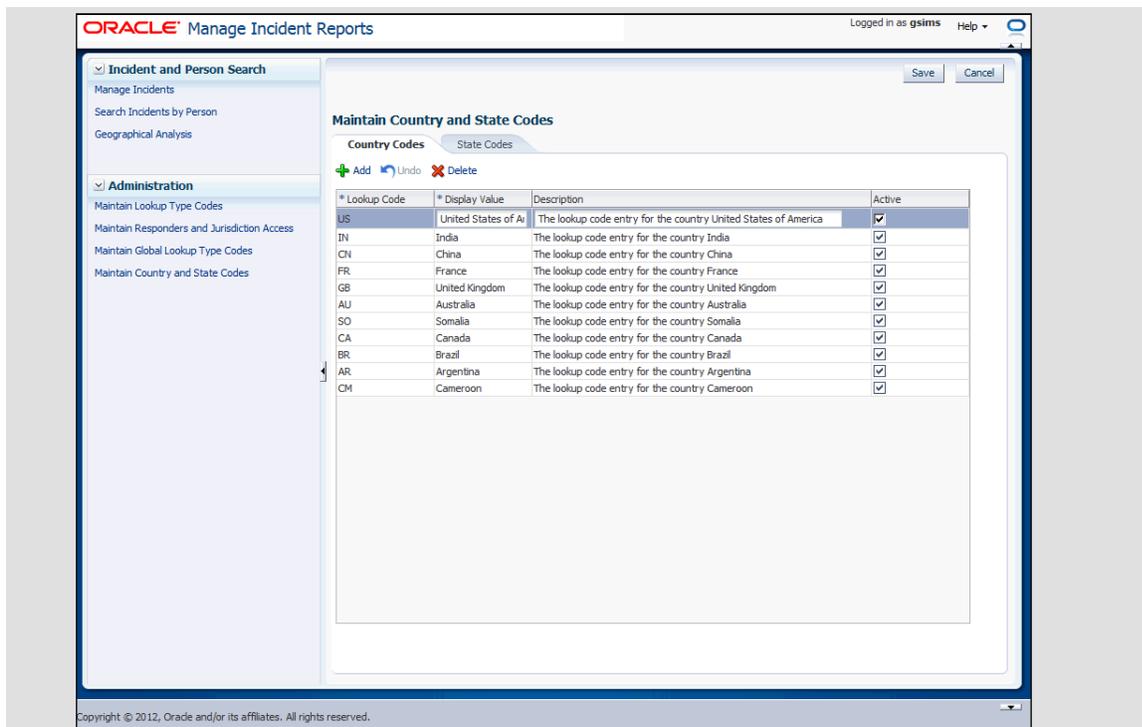
- Argentina
- Australia
- Brazil
- Cameroon
- Canada
- China
- France
- India
- Somalia
- United Kingdom
- United States of America

You can add additional country codes to meet your organization's needs.

In this topic, you will modify options for country codes.

#### ***Procedure: Maintaining Country Codes***

1. Begin by navigating to the **Maintain Country and State Codes** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Country and State Codes** link.
4. Use the **Maintain Country and State Codes** page to modify the country and state codes made available when creating or reviewing an incident report.
5. Use the **Country Codes** tab to modify the country codes made available when creating or reviewing an incident report.



6. First, add a country code.  
Click the **Add** button.
7. **Lookup Codes** are unique keys in the data tables and built into the logic of Oracle PSIR.  
Click in the **Lookup Code** field.
8. A **Lookup Code** can be upper or lower case.  
Enter the desired information into the **Lookup Code** field. Enter "**SG**".
9. Next, specify a short display value. Display values appear when an incident report is created or reviewed.  
Click in the **Display Value** field.
10. Enter the desired information into the **Display Value** field. Enter, "**Singapore**".
11. Use the **Description** field to add an optional description.  
Click in the **Description** field.
12. Enter the desired information into the **Description** field. Enter "**The lookup code entry for the country Singapore**".
13. Saving the country code makes it available when you create or review incident reports.  
Click the **Save** button.
14. The country code **Singapore** is now added.
15. Next, modify the **Singapore** country code by editing the description.

Click in the **Description** field.

16. Enter the desired information into the **Description** field. Enter "**Singapore**".

17. You can reverse any modifications to a single selected row using the **Undo** button. To save the modification, you would click **Save** instead.

Click the **Undo** button.

18. There are two types of delete, a hard delete and soft delete.

A hard delete removes the country code from the database table, provided it is not used in an incident report.

First, perform a hard delete on the code **Singapore**.

Click an entry in the row.

19. Click the **Delete** button.

20. Confirm that you want to delete the **Singapore** country code.

Click the **Yes** button.

21. Click the **Save** button.

22. The country code **Singapore** is now deleted.

23. A soft delete inactivates a country code already used in incident reports. Inactivated codes are not displayed as options for creating or reviewing incident reports.

Next, perform a soft delete on the **Cameroon** code.

Click an entry in the row.

24. Click the **Active** option.

25. Click the **Save** button.

26. The country code **Cameroon** is now inactive.

27. You have completed the **Maintaining Country Codes** topic.

### ***Maintaining State Codes***

State codes enable a reporter or citizen to specify the state where the incident occurred. Oracle Public Sector Incident Reporting ships with seeded values for state codes. The seeded values are:

Argentina

- Buenos Aires Province
- Catamarca Province
- Chaco Province
- Chubut Province
- Mendoza Province

Australia

- Northern Territory
- South Australia
- Tasmania
- Western Australia
- Victoria

Brazil

- Acre
- Amazonas
- Bahia
- Rio de Janeiro
- Alagoas

Cameroon

- Awing
- Babungo
- Bakossi

Canada

- Alberta
- British Columbia
- Saskatchewan
- Quebec
- Ontario

China

- Anhu
- Fujian
- Shandong
- Henan
- Shaanxi

France

- Alsace
- Aquitaine
- Picardy
- Burgundy

- Upper Normandy

#### India

- Karnataka
- Maharashtra
- West Bengal
- Tamil Nadu
- Uttar Pradesh

#### Somalia

- Somaliland
- Puntland
- Galmudug

#### United Kingdom

- Essex
- Derbyshire
- Lincolnshire
- Nottinghamshire
- Surrey

#### United States of America

- California
- Arizona
- Florida
- Texas
- New York

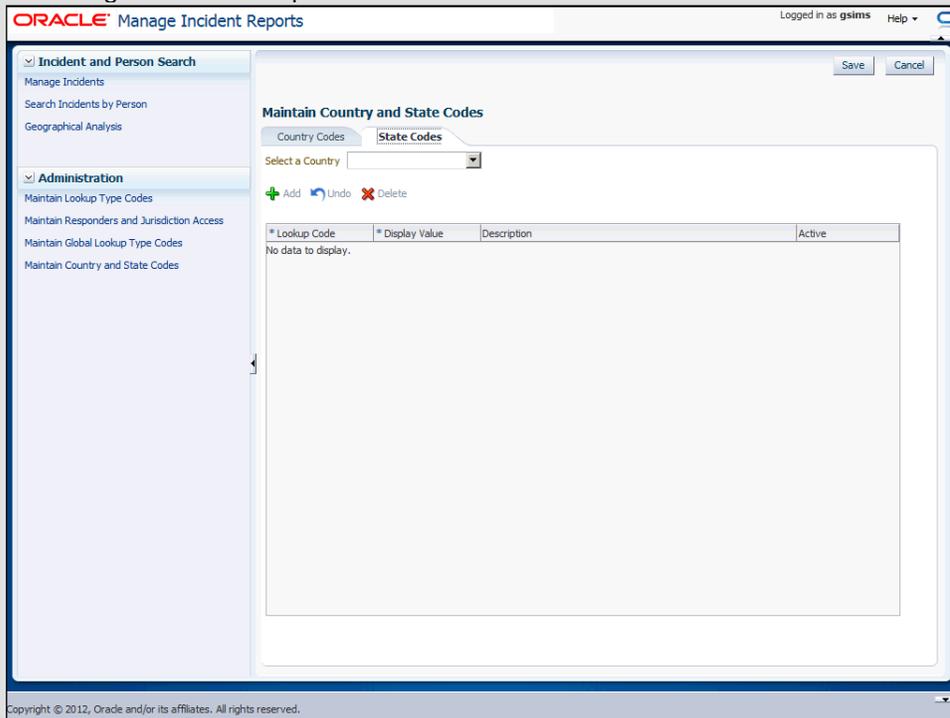
You can add additional state codes to meet your organization's needs.

In this topic, you will modify options for state codes.

#### ***Procedure: Maintaining State Codes***

1. Begin by navigating to the **Maintain Country and State Codes** page.  
Click the **Links** link.
2. Click the **Manage Incident Reports** link.
3. Click the **Maintain Country and State Codes** link.
4. Use the **Maintain Country and State Codes** page to modify the country and state codes made available when creating or reviewing an incident report.

5. Click the **State Codes** tab.
6. Use the **State Codes** tab to modify the states codes made available when creating or reviewing an incident report.



7. First, select a country to add the state code to.  
Click the **Select a Country** list.
8. Click the **United States of America** list item.
9. Click the **Add** button.
10. **Lookup Codes** are unique keys in the data tables and built into the logic of Oracle PSIR.  
Click in the **Lookup Code** field.
11. A **Lookup Code** can be upper or lower case.  
Enter the desired information into the **Lookup Code** field. Enter "**CO**".
12. Next, specify a short display value. Display values appear when an incident report is created or reviewed.  
Click in the **Display Value** field.
13. Enter the desired information into the **Display Value** field. Enter "**Colorado**".
14. Use the **Description** field to add an optional description.  
Click in the **Description** field.
15. Enter the desired information into the **Description** field. Enter "**The lookup code entry for the state of Colorado**".

16. Saving the state code makes it available when you create or review incident reports.

Click the **Save** button.

17. The state code **Colorado** is now added.

18. Next, modify the **Colorado** state code by editing the description.

Click in the **Description** field.

19. Enter the desired information into the **Description** field. Enter "**Colorado**".

20. You can reverse any modifications to a single selected row using the **Undo** button. To save the modification, you would click **Save** instead.

Click the **Undo** button.

21. There are two types of delete, a hard delete and soft delete.

A hard delete removes the state code from the database table, provided it is not used in an incident report.

First, perform a hard delete on the code **Colorado**.

Click an entry in the row.

22. Click the **Delete** button.

23. Confirm that you want to delete the **Colorado** state code.

Click the **Yes** button.

24. Click the **Save** button.

25. The state code **Colorado** is now deleted.

26. A soft delete inactivates a state code already used in incident reports. Inactivated codes are not displayed as options for creating or reviewing incident reports.

Next, perform a soft delete on the **New York** code.

Click an entry in the row.

27. Click the **Active** option.

28. Click the **Save** button.

29. The state code **New York** is now inactive.

30. You have completed the **Maintaining State Codes** topic.

## Understanding Oracle Public Sector Incident Reporting Business Rules

This section is intended for administrators who maintain Oracle Public Sector Incident Reporting (PSIR).

Oracle Public Sector Incident Reporting ships with seeded data for business rules. This section covers the business rules you can modify.

Upon completion of this section, you will be able to:

- Describe the Determine Incident Type Priority Ruleset.
- Describe the Determine Location Type Priority Ruleset.
- Describe the Calculate Incident Priority Ruleset.
- Describe the Search Similar Incidents Ruleset.
- Describe the Compare Incident Threshold Ruleset.
- Describe the Get Approvers Ruleset.

**Understanding the Determine Incident Type Priority Ruleset**

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses the Incident Type Priority Matrix Decision Table, in the Determine Incident Type Priority Ruleset, to determine the priority for each incident type. This decision table includes conditions and actions as its rows and rules as its columns. The rules test the values of the conditions and set corresponding values for the actions. The rules must account for all possible combinations of values of all conditions in the table. A value of otherwise means "all values not listed." Bucketsets and globals are used to set pre-defined values for certain rules.

Upon submission of an incident report, the rules engine tests each condition. If a combination of condition values matches a rule, the corresponding actions are taken. The Incident Type Priority Matrix Decision Table provides the details for each condition, its rules, and the actions to execute. Following the table is an example scenario explaining how an incident report is processed based on the given condition.

**Incident Type Priority Matrix Decision Table**

		R1	R2	R3
<b>Conditions</b>	RecommendActionBOType.incidentType	otherwise; Burglary; Car Jacking; Cyber Attack; Drug Related Activity; Emotionally Disturbed Person; Materials Acquisition; Observation/Surveillance; Traffic Accident; Weapons Discovery	Arson; Assault; Homicide; Public Health Threat	Fraud; Graffiti; Graffiti, Political
<b>Actions</b>	assert new IncidentTypePriorityFact Priority:int	✓ Medium Priority	✓ Arson	✓ Fraud

Reports are called in on a car selling drugs in front of a school. The Incident Type Priority is set to 2 because the Drug Related Activity global is 2.

To change the Incident Type parameters, change the values of the various Incident Type globals. By default, the values range from 1 to 3, highest to lowest.

You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

**Understanding the Determine Location Type Priority Ruleset**

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*

- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses the Location Type Priority Matrix Decision Table, in the Determine Location Type Priority Ruleset, to calculate the priority of an incident's location. This decision table includes conditions and actions as its rows and rules as its columns. The rules test the values of the conditions and set corresponding values for the actions. The rules must account for all possible combinations of values of all conditions in the table. A value of otherwise means "all values not listed. Bucketsets and globals are used to set pre-defined values for certain rules.

Upon submission of an incident report, the rules engine tests each condition. If a combination of condition values matches a rule, the corresponding actions are taken. The Location Type Priority Matrix Decision Table provides the details for each condition, its rules, and the actions to execute. Following the table is an example scenario explaining how an incident report is processed based on the given condition.

**Location Type Priority Matrix Decision Table**

Conditions	RecommendActionBOType.LocationType	R1	R2	R3	R4
		otherwise; Business; Business Park; Highway; Industry; Mall; Private Home; Street	Government Building; Hospital; School; Public Building	Open Area; Park	""
Actions	assert new LocationTypePriorityFact priority:int	✓	✓	✓	✓
		Medium Priority	Government Building	Open Area	Default Priority

Reports are called in on a car selling drugs in front of a school. The Location Type Priority is set to 1 because the School global is 1.

To change the priority parameters, change the values of the High Priority, Medium Priority, Low Priority, and Default Priority globals. By default, the values are 1, 2, 3, and 10 respectively.

You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

**Understanding the Calculate Incident Priority Ruleset**

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses the Incident Priority Matrix Decision Table, in the Calculate Incident Priority Ruleset, to calculate the priority of an incident. The priority of an incident is based on its type and location where the incident occurred. This decision table includes conditions and actions as its rows and rules as its columns. The rules test the values of the conditions and set corresponding values for the actions. The rules must account for all possible combinations of values of all conditions in the table. Bucketsets and globals are used to set pre-defined values for certain rules.

Upon submission of an incident report, the rules engine tests each condition. If a combination of condition values matches a rule, the corresponding actions are taken. The Incident Priority Matrix Decision Table provides the details for each condition, its rules, and the actions to execute. Following the table is an example scenario explaining how an incident report is processed based on the given condition.

**Incident Priority Matrix Decision Table**

		R1	R2
<b>Conditions</b>	IncidentTypePriorityFact.priority <= LocationTypePriorityFact.priority	true	false
<b>Actions</b>	assert new IncidentPriorityBOType priority:Integer	✓	✓
		IncidentTypePriorityFact.priority	LocationTypePriorityFact.priority

A delivery driver spots and reports an incident where some young kids are spraying graffiti on the back of the mall. The Graffiti Incident Type Priority is a 3, the mall has a Location Type Priority of 2. The incident priority is set to a 2.

To change the priority parameters, change the values of the Incident Type Priority or Location Type Priority globals. By default, the priority values range from 1 to 3, highest to lowest. You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

**Understanding the Search Similar Incidents Ruleset**

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses Rule 1, Rule 2, Rule 3, Rule 4, and Rule 5 in the Search Similar Incidents Ruleset, each of which includes a condition (IF) statement and an action (THEN) statement. Bucketsets and globals are used to set pre-defined values for certain rules.

The condition of Rule 1 specifies that the current incident type is not Arson and is not Burglary. The action sets search parameters to null and does not search for similar incidents.

The condition of Rule 2 specifies that the current incident type is Arson or Burglary and that the default city and state to be searched are not specified. The action searches for similar incidents based on the current incident city and globals that specify the Incident Severity, Incident State, number of Prior Days, within the Proximity Radius, and DistanceUnit.

The condition of Rule 3 specifies that the incident type is Arson or Burglary and that the default city to be searched is not specified but the state is specified. The action searches for similar incidents based on globals that specify the Incident City, Incident Severity, Incident State, number of Prior Days, within the Proximity Radius, and DistanceUnit.

The condition of Rule 4 specifies that the incident type is Arson or Burglary and that the default city to be searched is specified but the state is not specified. The action searches for similar incidents based on globals that specify the Incident City, Incident Severity, Incident State, number of Prior Days, within the Proximity Radius, and DistanceUnit.

The condition of Rule 5 specifies that the incident type is Arson or Burglary and that the default city and state are specified. The action searches for similar incidents based on globals that specify the Incident City, Incident Severity, Incident State, number of Prior Days, within the Proximity Radius, and DistanceUnit.

To change the search parameters, change the values of the Incident City, Incident Severity, Incident State, and Prior Days globals. By default, Prior Days is set to 1 and the other parameters are not specified (set to empty strings). You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset

is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

### Understanding the Compare Incident Threshold Ruleset

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses the Compare Incident Threshold Matrix Decision Table, in the Compare Incident Threshold Ruleset, to determine whether a sufficient number of incidents are similar enough to be related. This decision table includes conditions and actions as its rows and rules as its columns. The rules test the values of the conditions and set corresponding values for the actions. The rules must account for all possible combinations of values of all conditions in the table. Bucketsets and globals are used to set pre-defined values for certain rules.

Upon submission of an incident report, the rules engine tests each condition. If a combination of condition values matches a rule, the corresponding actions are taken. The Compare Incident Threshold Matrix Decision Table provides the details for each condition, its rules, and the actions to execute. Following the table is an example scenario explaining how an incident report is processed based on the given condition.

#### Compare Incident Threshold Matrix Decision Table

		R1	R2
<b>Conditions</b>	CompareIncidentThreshold.in.compareIncidentType >= Incident Threshold	true	false
<b>Actions</b>	assert new RelateIncidentBOType	✓	✓
	relateIncident:String	"Y"	"N"

The Incident Threshold is set to three and there have been four arson incidents in the same city in the last 24 hours. These arson incidents are flagged as related.

To change the Incident Threshold, reset the Incident Threshold global. By default, Incident Threshold is set to 2.

For details about the comparison logic that determines incident similarity, see Understanding the Search Similar Incidents Ruleset.

You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

### Understanding the Get Approvers Ruleset

You must have a solid working knowledge of Oracle SOA Suite, Oracle BPM Suite, and Oracle Business Rules before modifying any business rules. For information on these products, see:

- *Oracle Fusion Middleware User's Guide for Oracle Business Rules*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA and Oracle Business Process Management Suite*

Oracle Public Sector Incident Reporting uses the Approval Matrix Decision Table, in the Get Approvers Ruleset, to determine the personnel to whom an incident report is assigned based on the incident type. This decision table includes conditions and actions as its rows and rules as its columns. The rules test the values of the conditions and set corresponding values for the actions. The rules must account for all possible combinations of values of all conditions in the table. A value of otherwise means all values not listed. Bucketsets are used to set pre-defined values for certain rules.

Upon submission of an incident report, the rules engine tests each condition. If a combination of condition values matches a rule, the corresponding actions are taken. The Approval Matrix Decision Table provides the details each condition, its rules, and the actions to execute. Following the table is an example scenario explaining how an incident report is processed based on the given condition.

**Approval Matrix Decision Table**

Conditions		R1	R2	R3	R4	R5	R6
ReviewIncidentPayload Type.reportIncidentData incidentData.incident Type		otherwise	Arson	Cyber Attack	Drug Related Activity	Material Acquisition	Observation/Surv eillance
Actions	call CreateResourceList	✓	✓	✓	✓	✓	✓
	users:String	null	null	null	null	null	null
	groups:String	null	null	null	null	null	null
	approles:String	"ActionOfficer- OtherIncidents"	"ActionOfficer- Arson"	"ActionOfficer- CyberAttack"	"ActionOfficer- DrugRelated"	"ActionOfficer- MaterialAcquisiti on"	"ActionOfficer- Observation"
	responseType:Resp onseType	ResponseType.RE QUIRED	ResponseType.RE QUIRED	ResponseType.RE QUIRED	ResponseType.RE QUIRED	ResponseType.RE QUIRED	ResponseType.RE QUIRED
	ruleName:string	"Other Incidents Approver"	"ArsonIncidentA pprover"	"Cyber Incident Approvers"	"Drug Incident Approvers"	"Material Acquisition Incident Approvers"	"Observation Incident Approvers"
	lists:Lists	Lists	Lists	Lists	Lists	Lists	Lists

An Arson type incident is reported. An action officer with the Arson incident type assignment is given the task of arranging for the city fire department to put out the fire and investigate the cause.

You can modify the existing ruleset, conditions, or actions. Take caution before modifying a condition or action, it can require source code changes. Incident processing fails if this ruleset is deleted. To modify the ruleset, conditions, or actions, see "Editing Rules in an Oracle Business Rules Dictionary at Run Time," in *Oracle Fusion Middleware User's Guide for Oracle Business Rules*.

**Understanding Oracle Public Sector Incident Reporting Reports**

This section is intended for case managers and department managers reviewing reports.

You must have a solid working knowledge of Oracle Business Activity Monitoring (BAM) before creating or editing the Oracle Public Sector Incident Reporting (PSIR) dashboards and reports. For information on creating and editing Oracle BAM reports, see "Creating and Managing Reports," in *Oracle Fusion Middleware User's Guide for Oracle Business Activity Monitoring*.

This section covers the Oracle BAM dashboard and reports delivered with Oracle PSIR. Oracle Public Sector Incident Reporting includes one dashboard, the Incident Reporting Dashboard, with two reports. These reports use information from the incident reports submitted in Oracle PSIR. Information from saved incident reports is not used in the reports.

**Incident Reporting Dashboard**

The Incident Reporting dashboard has two reports - The Incident Activity Monitoring Report and the Incident Analytics Report. Each of these reports has five views pertaining to the type and location of the incidents reported. You can filter the views using the report parameters Incident Type and Incident Location on the Incident Activity Monitoring Report and the parameters Time Period and Incident Location for the Incident Analytics Report. The following provides an explanation and a sample image of the reports and views.

**Incident Activity Monitoring**

The Incident Activity Monitoring Report contains views from real-time monitoring of the incident reporting business processes to make sure they are run smoothly. This report has five views.

Streaming List

The Streaming List provides a list of Incident Types like Arson, Burglary, Car Jacking and so on. Adjacent to this field are the fields: Incident Date, Incident City, Incident Postal Code, Incident State, and Incident Status.

Streaming List					
Incident Type	Incident Date	Incident City	Incident Po...	Incident State	Incident St...
Arson	1/11/2013 2:08	Oakland		California	Open
Assault	1/11/2013 5:20	Oakland		California	Open
Arson	1/11/2013 5:23	Newyork		New York	Open
Arson	1/11/2013 5:26	Oakland		California	Open
Arson	2/6/2013 9:58:0	Oakland		California	Open

Number of Incidents List

The Number of Incidents List is a view of each Incident Type and the number of times it has been reported. The view displays the Incident Type in alphabetical order in the extreme left column and towards the right, the frequency of each incident type by day, last seven days, the current month, Year To Date (YTD), and a comparison of frequencies for the day with Last Year Same Day.

Number of Incidents List					
Incident Type	Today	Last 7 Days	This Month	YTD	Last Year S...
Arson	1	19	20	28	0
Assault	0	0	0	4	0
Burglary	0	1	1	1	0
Cyber Attack	2	2	2	2	0
Emotionally Dist	0	1	1	1	0
Fraud	0	1	1	1	0
Car Jack	0	0	0	0	0

Action List

The Action List view displays a list of Too many Open Incidents for the past 24 hours with columns for Message Text, Received Date, and Subject Text from left to right. You can edit the report to view too many open incidents for Homicide using BAM Active Studio.

Action List			
MessageText	ReceivedDate	SubjectText	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 41	2/11/2013 4:38:24 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 41	2/11/2013 4:35:06 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 40	2/11/2013 4:16:30 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 40	2/11/2013 4:15:58 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 39	2/11/2013 4:06:01 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 39	2/11/2013 3:59:27 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 38	2/11/2013 3:41:48 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 38	2/11/2013 3:39:05 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 37	2/10/2013 8:16:23 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 37	2/10/2013 8:16:09 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 36	2/10/2013 8:10:11 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 36	2/10/2013 8:09:53 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 35	2/10/2013 8:08:04 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 35	2/10/2013 8:07:49 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 34	2/10/2013 8:05:27 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 34	2/10/2013 8:04:56 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 33	2/10/2013 7:51:54 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 33	2/10/2013 7:51:31 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 32	2/8/2013 11:33:11 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 31	2/8/2013 11:31:33 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 30	2/8/2013 11:30:35 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 29	2/8/2013 11:10:09 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 30	2/8/2013 4:20:47 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 30	2/8/2013 4:13:05 AM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 29	2/6/2013 11:59:11 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 30	2/6/2013 11:57:16 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 30	2/6/2013 11:56:22 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 29	2/6/2013 11:54:34 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 29	2/6/2013 11:51:38 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 28	2/6/2013 11:37:23 PM	Too many Open Incidents : Email Too many Open Incidents	
<input type="checkbox"/> Too many Open Incidents Number of Incidents: 28	2/6/2013 11:36:57 PM	Too many Open Incidents : Email Too many Open Incidents	

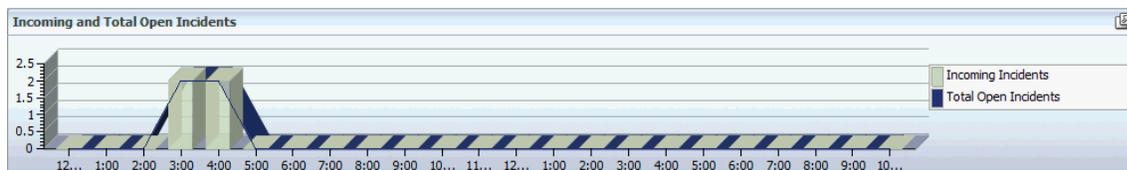
Incident Type by City

The Incident Type by City is a crosstab view that displays the count of each incident type in each city. From the left, vertical rows for each incident type are listed alphabetically. To the right are columns for each city with the number of incidents per incident type. A count column at the far right tallies the total number of incidents per type and a grand count row at the bottom provides the total number of incidents per city. You can filter the view to show specific selected incidents or cities.

Incident Type by City					
# of Incidents (Count)					
Incident City					
Incident Type	Almaeda	Bangaloe	Bangalore	DALLAS-FORT WORTH	
	# of Incidents	# of Incidents	# of Incidents	# of Incidents	# of Incidents
Arson	1	3		1	
Assault					
Burglary					
Cyber Attack					
Emotionally Disturbed Person					
Fraud					
Graffiti		2			
Homicide					
Materials Acquisition			1		
Public Health Threat					
Grand Count	1	5	1	1	

Incoming and Total Open Incidents

The Incoming and Total Open Incidents view is a 3D Combo Chart showing both incoming and open incidents. The line chart shows the open incidents and the bar chart shows incoming incidents. Only incidents opened within the day are shown. The X-axis maps the time through one hour intervals and the Y-axis maps the number of incidents.

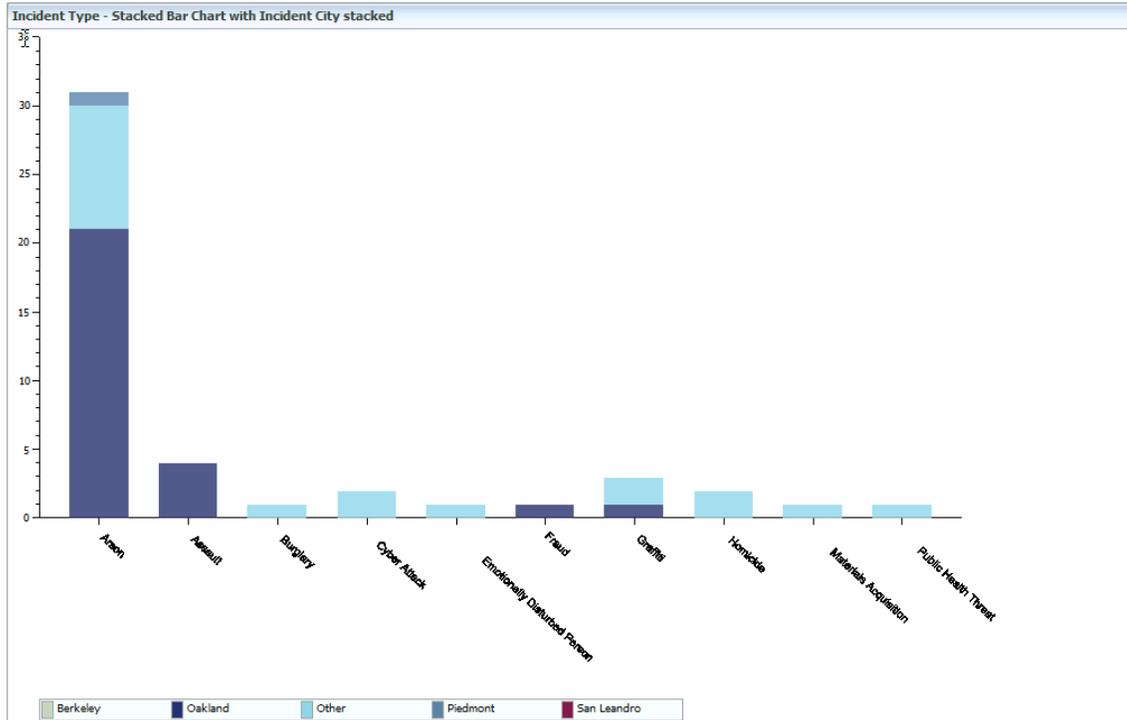


**Incident Analytics**

The Incident Analytics report provides the historical analysis of the incident reporting business process. This report has five views.

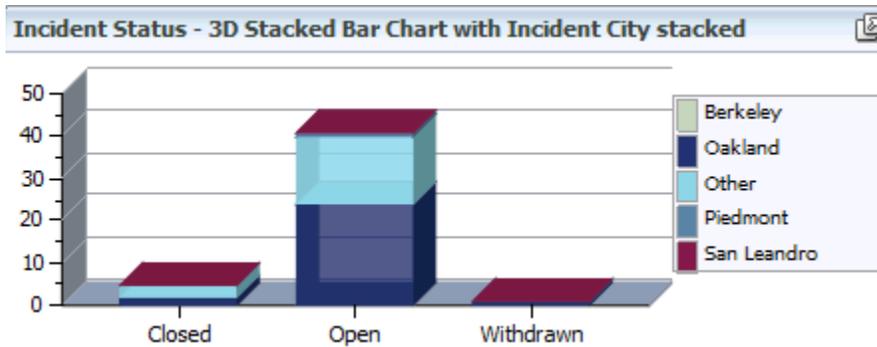
**Incident Type - Stacked Bar Chart with Incident City Stacked**

The Incident Type view displays a bar chart that maps the frequency of incident types with the incident city stacked together in bars. The X-axis maps the incident types in alphabetical order from left to right. The Y-axis maps the frequency of incident types from zero to infinity with the interval width of five incidents.



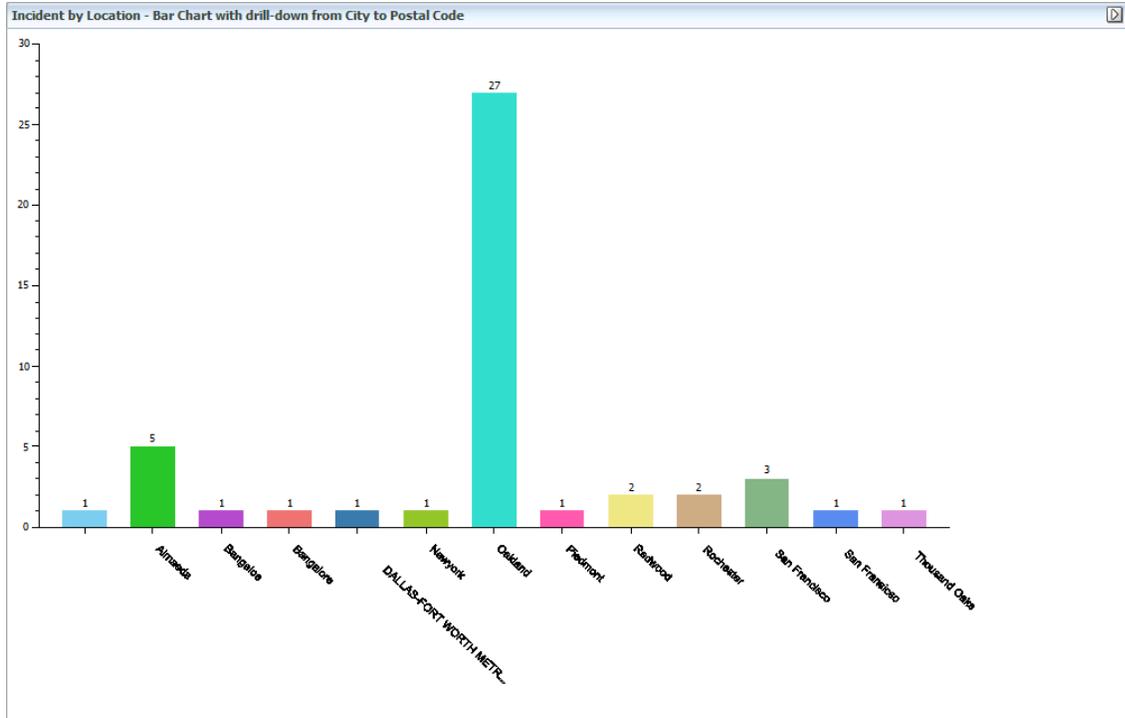
**Incident Status - 3D Bar Chart with Incident City Stacked**

The Incident Status 3D bar chart displays the incident status of all incident reports within the chosen time range with the statuses: Closed, Invalid, New, Open, and Withdrawn. These are mapped on the X-axis and the number of incident reports is mapped on the Y-axis with the interval width of 20 incident reports. The incident cities are separated by bars stacked upon each other on the X-axis.



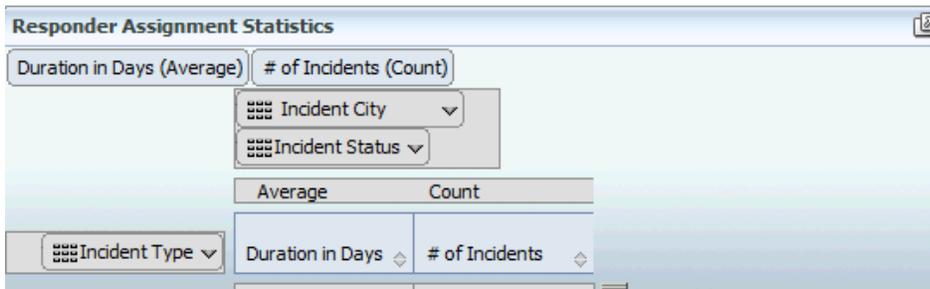
**Incident by Location - Bar Chart with Drill-Down from City to Postal Code**

The Incident by Location view displays a bar chart with incident locations mapped on the X-axis and the frequency of incidents on the Y-axis from zero to infinity with the interval width of five incidents on the chart. You can apply filters and drill down to specific cities for any comparison. Clicking the bars will break the incidents for that city down into incidents by postal code.



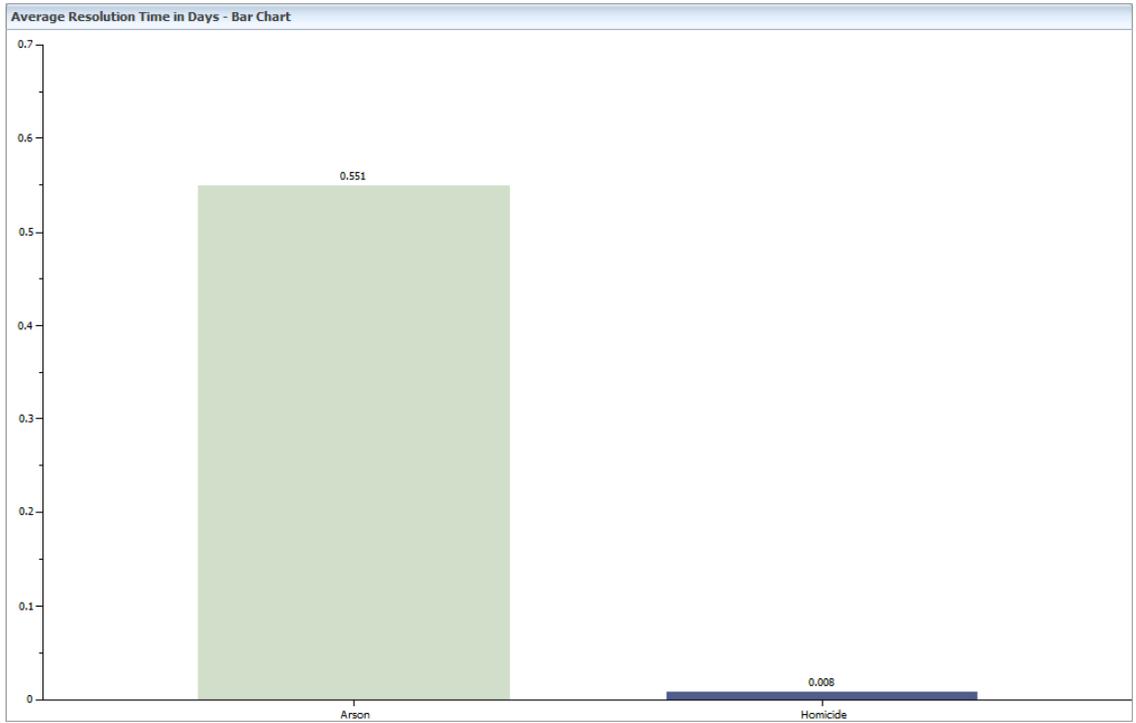
Responder Assignment Statistics

The Responder Assignment Statistics is a crosstab view that displays the average and total time taken to assign a responder to incident reports sorted by each incident type. To the far left is the Incident Type column with the incident types arranged alphabetically. This column is followed by the columns for specific incident locations with counts and averages spread across towards the right. You can filter the view to show specific selected incidents or cities.



Average Resolution Time in Days

The Average Resolution Time in Days view is a bar chart that displays the average time in days for each incident from the time when it is reported to when it is closed. The X-axis shows the incident types alphabetically from left to right with the exact number of days for which the incident has been opened, on the top of each bar. The Y-axis shows the average time in days starting at 0 to infinity with the interval width of two days until the incident is closed.



## Delivered Documentation

This section provides a complete list of the delivered documentation for Oracle Public Sector Incident Reporting (PSIR).

The delivered documents are:

**Oracle Fusion Middleware Installation Guide for Oracle Process Accelerators** - This content provides instructions for installing any Oracle Process Accelerator.

**Oracle Fusion Middleware Extensibility Guide for Oracle Process Accelerators** - This content provides information about customizing and extending Oracle Process Accelerators.

**Oracle Process Accelerators Known Issues** - This content provides information about the known issues with any Oracle Process Accelerator.

**Oracle Fusion Middleware User's Guide for Oracle Public Sector Incident Reporting Process Accelerator** - This content provides information on how to use and modify Oracle Public Sector Incident Reporting Process Accelerator. The content of this manual is also available in the following formats:

- Process Accelerator Help system
- User Productivity Kit (UPK) demo
- UPK source content

**Process Accelerator Help System** - The Help system is available when you launch the  or the **User Productivity Kit** link from the process accelerator Help menu.

**UPK Demo** - You can use the User Productivity Kit demo for training or presentation purposes while installing the process accelerator. To utilize the UPK demo, unzip the **PAacronymUPKDemo.zip** file and distribute the PlayerPackage directory and its contents to those who need training; or place the PlayerPackage directory and its contents on a web server and provide the URL to its location. The **play.exe** file launches the UPK Player.

**UPK Source Content** - If you have a licensed version of Oracle User Productivity Kit you can modify the UPK content using the **UPKSource.zip** file. Use the following steps to deploy your modified UPK content as the Help for the Process Accelerator.

1. Unzip **UPKSource.zip**.
2. In UPK Developer, import the **PAacronymUPKSourceContent.odarc** file you want to modify.
3. Modify and publish your updated content to the Player.
4. Rename the **PlayerPackage** directory to **PAacronymUPK**.
5. Convert the **PAacronymUPK** directory and its contents into a web application archive (war) file called **PAacronymUPK.war**.
6. On your Oracle WebLogic Server, navigate to **\$PA\_HOME/pa/src/PAacronym/UPKObjects**, rename **PAacronymUPK.war** to **PAacronymUPK.warORIG**.
7. Copy your new **PAacronymUPK.war** to **\$PA\_HOME/pa/src/PAacronym/UPKObjects**.
8. Navigate to **\$MW\_HOME/user\_projects/domains/soainfra/servers/AdminServer/upload/PAacronymUPK/app**, rename **PAacronymUPK.war** to **PAacronymUPK.warORIG**.
9. Copy your new **PAacronymUPK.war** to **\$MW\_HOME/user\_projects/domains/soainfra/servers/AdminServer/upload/PAacronymUPK/app**.

10. In Oracle WebLogic Server Administration Console, navigate to the **Domain Structure** navigation tree, click **Deployments**.
11. On the **Summary of Deployments** page, select the **PAacronymUPK** check box, and click **Update**.
12. On the **Update Application Assistant** page, change the **Source Path** to the location you extracted the **PAacronymUPK.war** file to.
13. Click **Next**, **Next**, then **Finish**.
14. Launch the Process Accelerator Help to view the updated documentation.