ORACLE

Oracle Label Security

Label Security uses row level data classifications to enforce access controls restricting users to only the data they are allowed to access. It enables organizations to control their operational and storage costs by enabling data with different levels of sensitivity to co-mingle within the same database.

June 11, 2020

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in latest releases of Oracle Label Security. It is intended solely to help you assess the business benefits of using Oracle Label Security preventive controls and to plan your Data Security / I.T. projects.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Table of Contents

INTRODUCTION

Over the past 40 years, Oracle has been the industry leader in building innovative data security solutions that make it possible to protect sensitive information. Oracle Label Security (OLS) is part of Oracle's defense-in-depth approach to security and is the industry's most advanced solution for controlling access to data based on data classification. While this technology was designed to meet US government, military and intelligence agency standards, OLS is also applicable to commercial organizations that have data separation requirements for their users. Both government and commercial organizations use OLS to consolidate multiple databases to reduce operational costs as well as simplifying data analysis and decision-making. Government agencies align their data classification standards and then use OLS to share data across agencies. Commercial companies use OLS to separate data from different nationalities, allowing users from different countries to access data and meet local privacy and compliance requirements. Other companies are consolidating similar databases from subsidiaries and retail outlets and require limits on what is visible to each group. Oracle Label Security has out of the box features to enable these and similar use cases.

Oracle Label Security mediates access based on data sensitivity labels (referred to in this document as data labels) and user label authorizations (referred to in this document as user labels). Oracle Label Security has consistently been evaluated as part of the Oracle Database to the Common Criteria for Information Technology Security Evaluation (ISO15408) as part of the Oracle Database. Oracle Label Security is easily managed by using either the API calls or Oracle Enterprise Manager. Oracle Label Security is an option available with Oracle Database Enterprise Edition, and it is included with the High Performance and Extreme Performance Editions of Oracle Database Cloud Service, on the Autonomous Cloud Databases and on Oracle Exadata Cloud Service.

ORACLE LABEL SECURITY CONCEPTS

The need for more sophisticated controls on application access to sensitive data is becoming increasingly important as organizations address emerging security requirements around data consolidation, privacy, and compliance. Maintaining separate databases for highly sensitive data (projects, HR, finance) is costly and creates unnecessary administrative overhead. However, consolidating databases sometimes means combining sensitive data from different databases in one system. Oracle Label Security provides the ability to tag data with a data label or a data classification. This capability allows the database to inherently know what data is appropriate for each user and enforce security controls. Data can also be labeled with a degree of sensitivity (known as a level). For example, in government and defense applications, data might be labeled unclassified, secret, or top secret, while in a healthcare application it may be labeled public, confidential, restricted, or highly restricted.

Oracle Label Security enforces access controls by comparing a data classification label with a user's access clearance. Access clearance can be thought of as an extension to standard database privileges and roles. For example, a very common database operation is to grant select on an application table to a user or a role. With this privilege, the user or role can select all the rows in the table. To restrict access to highly sensitive data rows, two things must take place: First, the database must know what data is considered highly sensitive. Second, the database has to know the access clearance of the user. Oracle Label Security solves this problem by providing the ability to define data classification labels, assign access clearances to users, assign data classification labels to data, and enforce access control. Historically the design approach used to achieve this type of functionality was based on database views, triggers, and lookup tables. However, that approach required extensive application changes and resulted in inconsistent implementations across applications. Oracle Label Security is built-in and enforced within the database, below the application layer, providing stronger security and eliminating the need for application views and triggers. This enforces the access rights across all applications that connect to the data including reporting and business intelligence tools that normally require their own security model.

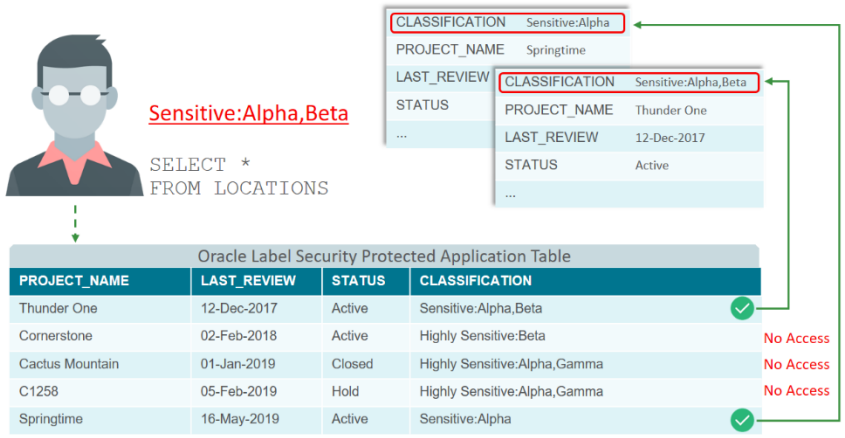

Figure 1: Oracle Label Security leverages user labels and data labels to control data access

Oracle Label Security is a mature product and can address simple to complex requirements. As with any other sophisticated security product, proper analysis and planning are key to a successful Oracle Label Security deployment. The steps below provide a basic guideline for deploying Oracle Label Security. The implementation can be performed using Oracle Enterprise Manager or the Oracle Label Security API. It may be useful to work with a sample demonstration table first to get a firm understanding of how data labels mediate access control as well as the various enforcement options available in Oracle Label Security.

Oracle Label Security Implementation Steps

STEPS
Perform the data analysis steps recommended in this paper
Create the Oracle Label Security policy
Define necessary data label components including levels, compartments, and groups
Provision user labels (Max, Min, Default)
Create the data labels for the policy using the components (levels, compartments, and groups) already defined
Apply the policy to the application tables. (Note that once applied, no data will be accessible unless special privileges have been granted to the user)
Update legacy data with appropriate data labels

This paper focuses on the core components (data labels, user labels) before we discuss policies and data analysis steps.

Data Labels and Protected Objects

Data label components include levels, compartments, and groups. These components are used to create data labels as well as to assign user labels to database or application type users. Levels are ordered from more sensitive to less sensitive. Compartments are independent and used to segregate data within a given level. Groups are used to segregate data organizationally within a given level. Groups can have an inherited, or parent-child hierarchical relationships, where having access to the parent Group provides access to the child Group. A given data label must have exactly one Level, zero or more Compartments and zero or more Groups associated with it. For deployments using only Compartments or Groups, a single, default, Level will need to be created and used for user or data labels.

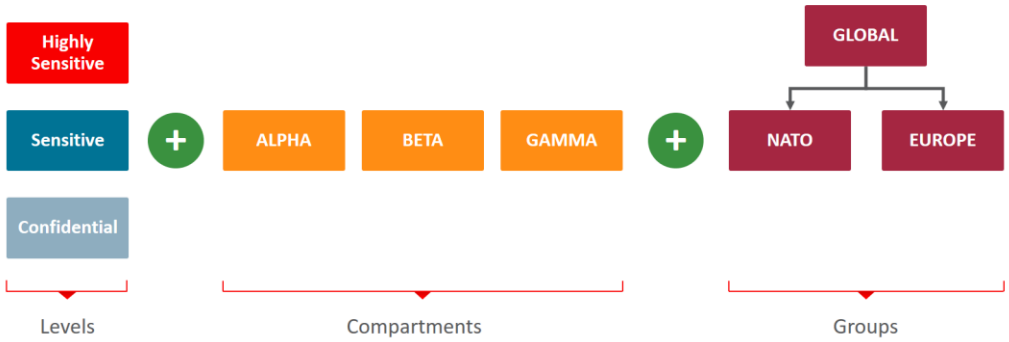

Figure 2. Oracle Label Security data levels can include levels, compartments and groups

Oracle Label Security - Data Label Components

LABEL COMPONENTS	DESCRIPTION
Level	The level is a component that denotes the sensitivity of the data. Every data and user label must have a level. An organization might define levels such as Confidential, Sensitive and Highly Sensitive. If an organization does not need multiple levels, a single default level needs to be defined.
Compartment	The compartment component is optional and is indepdenent of each other. Typically, one or more compartments are defined to compartmentalize data. Compartments might be defined for a specific type of data, knowledge area, geography, or project that requires special approval, such as HR, Finance, Accounting.
Group	The group component is optional and is very similar to a compartment except each group can have a parent-child relationship (hierarchy). Groups are most often used to segregate data by organizational structure or region, such as EU with child groups of France and Portugal or North America with child groups of US and Canada.

Examples of industry-specific policies and data labels

INDUSTRY	LEVEL	COMPARTMENT	GROUP
Government and Defense	Confidential Secret Top Secret	Desert Storm Border Protection	NATO Homeland Security
Law Enforcement	Level 1 Level 2 Level 3	Internal Affairs Drug Enforcement	Local Jurisdiction FBI Justice Department
Human Resources	Confidential Sensitive Highly Sensitive	PII Data Investigation	Global NA, Canada, USA EMEA, France, Portugal, Germany LATAM, Mexico, Brazil, Argentina
Health Care	Confidential Public	Patient Doctor	Lab_Technician Medical_Assistant
Retail Financials	Default*	None	Each Store, Country, Region, Financial Group
R&D	Default*	Project	Project Members, Project Lead, Corporate Finance, Corporate Legal

* While levels are not used to determine access for this use case, a level is required to be set.

Using Data Labels

The first and most important step in planning your Oracle Label Security deployment is determining your organization's data label requirements. This means determining what Levels, Compartments and/or Groups you require to protect your information. Determining your data label requirements generally means analyzing your application and identifying the tables that you plan to protect with Oracle Label Security. This is best accomplished with the assistance of an application administrator or developer who has knowledge of the application schema. In most cases, only a small percentage of the application tables will require an Oracle Label Security policy. Once the candidate tables have been identified, the data contained in the tables will need to be evaluated. The assistance of a data analyst, or someone with an understanding of the data, may be required. It is recommended that future application data is considered as well. This will create a robust set of initial label components.

Note that a single Oracle Label Security policy can have up 9999 levels and up to 9999 compartments and groups. However, many commercial organizations use only a single default level whereas a government or defense implementation might use between two and five levels.

The text-based representation of a data label uses colons and commas to separate the components. For example, the data label [Sensitive:Alpha,Beta:UK] contains the level (Sensitive), two compartments (Alpha and Beta), and one group (UK). The data label [Default::US] has the single required level called Default and the group US.

Internally, Oracle Label Security uses a numeric identifier called a label tag for each data label. Label tags are established when creating the data label. Label tags are stored with each row in a protected column defined by the administrator when a policy is created. The administrator can choose to have the column appended to an application table as a visible or invisible colum. Appending the column as an invisible column will eliminate any possibility of existing select, insert, or update statements failing because the SQL statement didn't qualify the names of the columns in the statement. It is important to note that the Oracle Label Security policy column can pre-exist in an application table prior to applying an Oracle Label Security policy. To take advantage of this, the application table column data type must be number (10). This allows applications to be designed with an Oracle Label Security policy column built-in.

When deciding whether to use compartments, groups or both, it is important to understand their differences with respect to required user authorization.

Required User Authorizations for Label Components

LABEL COMPONENTS	DESCRIPTION
Level	User must be authorized to the level or higher. For example, in order for a user to access data labeled “Sensitive”, the user must have been authorized to at least the “Sensitive” level. The number assigned to the level determines its ranking.
Compartment	User must be authorized to all compartments listed in the data label. For example, in order for a user to access data labeled “Sensitive: Alpha, Beta”, the user must have been authorized to at least the “Sensitive” level and to both the “Alpha” and “Beta” compartments. Unlike levels, the number assigned to a compartment has no meaning other than determining the display order of multiple compartments when using internal functions.
Group	User must be authorized to at least one of the groups listed in the data label or be authorized to a parent group. For example, for a user to access data labeled “Default::Canada”, the user must have been authorized to the Default level and the Canada group. But the parent of the Canada group is North America group so the North America group can also access the data. Note the colon separating the level, compartment and group sections in the label. Unlike levels, the number assigned to a group has no meaning other than determining the display order of multiple groups when using the label_to_char function or similar functions.

If the application has an entity-relationship (ER) diagram, it may be useful to annotate on the diagram the range of data labels for each entity.

User Labels

User labels determine whether a user can access information protected with a data label. User labels are comprised of a minimum and maximum level, a default level and a row level. In addition, user labels can have compartments and groups. For example, a user can be assigned a maximum level of Sensitive and a minimum level of Public. Database users also have a default label that is initialized when the user connects to the database. This is sometimes referred to as the active session label. The session label is simply the user’s current level combined with compartments and groups. The session label may differ from the user label based on rules that change it due to the connection. For example, even if a user has a Highly Sensitive level as part of their user label, if the connection is a remote session through VPN the session label may be restricted to the Sensitive level.

Oracle Label Security user labels must be established by the security administrator before an application user can access an application table protected by Oracle Label Security. Note that when multiple policies are present in the database, separate user authorizations must be established for each policy.

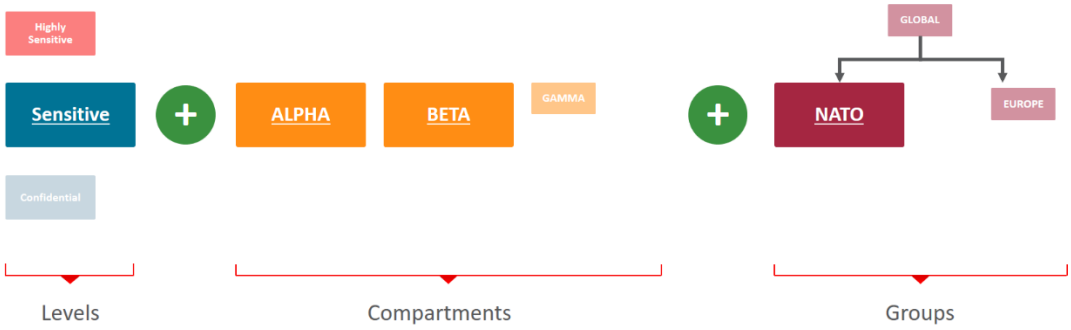

Figure 3: User Label Components include Levels, Compartments and Groups

Label Strategy

Defining a label strategy requires understanding the various roles and responsibilities of the user population. For example, a user might be designated as an analyst, highly privileged user, or administrative user. Understanding the various roles and responsibilities may require the assistance of managers and security administrators. After the user population has been separated into one or more roles or functional areas, a comparison needs to be performed between the data labels and the user label requirements. These need to correspond correctly for each of the tables identified earlier. This step is important to prevent data from being assigned a sensitivity label that no user has access to. In other words, the information required to perform a specific job responsibility might be out of reach to the application user due to his or her user label. In the worst case, data might be assigned a data label that no user can access, effectively hiding the data.

Sample Oracle Label Security authorization analysis

TABLE	DATA	USER			
		C	S	S:A:US	S:A,B:US,UK
Assets	C::UK	No Access	No Access	No Access	**Access**
	C::UK	No Access	No Access	No Access	**Access**
Projects	C	**Access**	**Access**	**Access**	**Access**
	S	No Access	**Access**	**Access**	**Access**
	S:A:US	No Access	No Access	**Access**	**Access**
	S:B:UK	No Access	No Access	No Access	**Access**
	S:A,B:US	No Access	No Access	No Access	**Access**

Review and Document

It is important that implementers review and document the information gathered. Include such information as a list of application tables that need to be protected, the reason why, as well as a list of label components and their meanings. This information will also be useful for applying other security controls as well such as Oracle Database Vault Realms or Command Rules, Oracle Data Redaction Policies, Oracle Data Masking Definitions, and Tablespace Encryption. This document should become part of the enterprise security policy and should be considered sensitive and kept in a safe location.

ORACLE LABEL SECURITY ADMINISTRATION

Installation Guidance

Oracle Label Security is installed by default with the Oracle Database, but it is not configured or enabled. You can configure and enable Oracle Label Security using the Oracle Database Configuration Assistant (DBCA) or through the command line. You should follow the steps provided in the documentation to create OLS policies, levels, compartments and/or groups.

If you are using a multitenant environment, only enable Oracle Label Security in the pluggable databases (PDBs) in which you plan to create OLS policies. Because OLS is not designed to protect data dictionary objects, you cannot create policies in the root.

Administering Users and Roles

The LBACSYS account contains the data dictionary that store Oracle Label Security policies, data labels, protected objects, enforcement settings, and user security clearances. LBACSYS stands for Label Based Access Control SYS. Beginning with Oracle 19c, LBACSYS, like other Oracle-provided accounts, is configured as a schema-only account. When you use OLS, the database security officer will need to run the ALTER USER command to provide a password to LBACSYS so the OLS administrator can access the account to grant LBAC roles to named users. Once the OLS administrator has completed granting roles, then the database security officer can run ALTER USER again to turn LBACSYS into a schema only account. Oracle recommends customers not use LBACSYS to manage Oracle Label Security since this is a shared account and will not be able to audit end-users correctly. As a good practice, for day-to-day use, grant the LBAC_DBA database role to trusted users who will administer Oracle Label Security.

Access to information stored in LBACSYS is controlled through policy specific roles and database views. Management of specific policies can be delegated to authorized individuals using Oracle Label Security specific database roles and by granting privileges on specific administrative packages. In addition to holding the metadata associated with Oracle Label Security, the LBACSYS account will also hold several dozen procedures and functions.

Delegated administration is possible using Oracle Label Security. When an Oracle Label Security policy “POLICYNAME” is created, a new database role POLICYNAME_DBA is also created. That role can then be used to manage policy label components and label authorizations and should be granted to a named user that is responsible to manage the policy.

Oracle Label Security Enforcement Exemptions

The following exceptions are important to understand when using Oracle Label Security policies.

Oracle Label Security enforcement exemptions

EXCEPTION	DESCRIPTION
SYS objects	Label Security policies cannot be applied to objects in SYS schema.
SYSDBA role	Any user that connects with the AS SYSDBA role is exempt from Label Security policies.
DIRECT path export	Label Security policies are not enforced during DIRECT path export.
EXEMPT ACCESS POLICY	Any user granted the Oracle Database EXEMPT ACCESS POLICY privilege directly, or through a database role, is exempt from Label Security policies.

Trusted Stored Procedures

A trusted stored program unit is created the same way that a standard procedure, function, or package is created. The program unit becomes trusted when you grant Oracle Label Security privileges to it. The Oracle Label Security privileges that can be granted to a user can also be granted to a trusted stored procedure. Doing so enables access to data within the execution context of a stored procedure but not directly by the user calling the stored procedure or function.

Oracle Label Security and Database Vault Capability

Many Oracle Label Security functions can be used within Oracle Database Vault rule sets to determine whether a user should be able to perform a specific operational task within the database. Using labels with Database Vault is an alternative use case for security clearances outside of pure data classification and provides for a finer grained separation of duty capability.

Oracle Label Security and Virtual Private Database Capability

Oracle Label Security also provides the ability to add an ad hoc restrictive 'where' clause or 'condition' when a policy is applied to an application table. This 'where' clause is used in conjunction with data labels to determine access and provides an easy to use, simple capability like creating an Oracle Virtual Private Database (VPD) policy. The 'where' clause is attached to the Oracle Label Security policy, thus there is no need to create a separate PL/SQL package as is the case with a pure VPD implementation.

Oracle Label Security and Data Redaction Policies

Oracle Label Security can also be used with Data Redaction to help decide if a redaction policy will be applied. For example, a Data Redaction policy can be applied where the Oracle Label Security user session label allows access to redacted or unredacted data.

Oracle Identity Management Integration

Oracle Label Security provides integration with Oracle Internet Directory. This feature enables centralized management of policy definitions, data labels and user label authorizations. Detailed information on Oracle Label Security and Oracle Internet Directory integration can be found in the Oracle Label Security Administrator's Guide.

BEST PRACTICES

Mapping Application Users to Database Users

Oracle Label Security supports common application architectures including "n-tier" applications that connect to the database using a single database account. To accomplish this, Oracle Label Security allows a session label to be set based on an application user instead of the database schema user. The application user's session label may be equal to the database user's session label or a subset of it. For example, instead of having access to multiple compartments and groups, the application user may have access to one Compartment and one Group.

Labeling Existing Data

If data labels have not been populated in the label tag for existing data, once an Oracle Label Security policy is applied to an application table no rows will be visible. This is because the label tag field will be NULL. You can optionally grant the administrator responsible for labeling the initial data the Label Security authorization FULL. This will allow the administrator to see all rows regardless of the data label and ensure that all existing data rows are property labeled.

The following are methods to apply data labels to existing data:

1. SQL UPDATE statements that populate the label tag of the controlled table based on the session label of the current user.

2. Use a database user with the session label required and populate the table with the data. If the OLS-controlled table has an active policy, the session label will be applied to the data as it is loaded. Oracle Data Pump could also be used with this method to import data from other databases.

3. Write a PL/SQL function to label the rows based on characteristics of the data and the context of the session.

Performance Considerations

Performance is important to all applications. Adding new functionality to existing applications requires careful planning, and due diligence to minimize the performance impact. Oracle Label Security enforces a security check on each row prior to allowing access, as well as during login authentication to initialize additional security contexts. The amount of delay will vary depending on the number of Oracle policies and the number of label components defined. The performance overhead will depend on a variety of factors including:

- Number of Oracle Label Security policies in place
- Number and size of tables protected by Oracle Label Security
- Oracle Label Security enforcement options used
- Complexity of existing or new application PL/SQL logic

Identifying the tables that require a Label Security policy is an important part of the upfront analysis. If all rows in a table are always accessed, applying a Label Security policy that assigns a data label to each row is not recommended and is probably redundant. Careful consideration of where to apply Label Security policies will result in an efficient use of the technology. In some cases, other Oracle Database security features may be more appropriate for addressing a given requirement than assigning a data label to each row. For example, if all rows are always accessed, using Oracle Database Vault to control when, where, why, and how a table is accessed may be more efficient than labeling every row. Regardless of the feature or functionality used, each additional security check performed will add additional performance overhead.

Oracle also recommends defining the associated label tags so that they fall within the range associated with the level of the data label. For example, suppose the levels Confidential and Sensitive have been defined along with two compartments, Alpha and Beta. The number associated with Confidential is 5000 and the number associated with Sensitive is 10000. When the valid data labels are defined the associated label tags associated with the level of Confidential and compartments Alpha and Beta should be between 5000 and 10000. For example, the data label Confidential:Alpha might have a label tag of 5050 and the data label Sensitive:Alpha,Beta might have a label tag of 10055.

Oracle Partitioning can be used with Oracle Label Security to physically partition data based on data classification. For example, data with a classification of Highly Sensitive can be located in a separate partition from data with a classification of Sensitive. Partitioning can also provide performance benefits through partition pruning, enabling Oracle Label Security to quickly skip data that resides outside of the users' security clearance. Partitioning is widely used in data warehouse

environments or applied to large tables where it provides query optimization through partition elimination and Oracle Label Security can leverage it as well. Oracle Label Security will quickly skip data that resides in partitions outside of the user's label.

Existing composite indexes can be modified to include the policy column added by Oracle Label Security. This can substantially improve performance for complex queries.

Should any user or stored procedure need access to all data it is recommended that the user or stored procedure be given the Oracle Label Security specific privilege READ or FULL. This will help reduce overhead and increase performance.

When labeling new data, using the LABEL DEFAULT enforcement policy option will have the least performance overhead.

Depending on the application usage, consideration should be given to creating bitmap indexes on the column added by Oracle Label Security to the application table. The percentage of unique labels compared to the number of data rows is usually low. Bitmap indexes will slow down data loads but increase performance on select statements.

CONCLUSION

Data classification plays a vital role not only in enforcing the principle of need-to-know but also in securely consolidating sensitive data. Historically, sensitive data has been stored in physically separate systems. However, this approach has limited the ability to perform advanced analysis and business intelligence.

Oracle Label Security provides the industry's most advanced and flexible data classification solution. Using a policy-based architecture, Oracle Label Security provides the ability to define data labels, assign security labels and protect application tables within the Oracle Database, reducing operational and storage costs by enabling different sets of data with different levels of sensitivity to reside in the same database. Oracle Label Security policies provide the ability to define custom data labels for virtually any industry ranging from healthcare to law enforcement to defense, reducing the cost of developing or re-coding applications to meet row level access control requirements based on clearance levels. Flexible enforcement options allow access control to be finely tuned to meet a variety of compliance and regulatory requirements.

Management of Oracle Label Security policies can be performed using Oracle Enterprise Manager and integration with Oracle Internet Directory provides centralized enterprise management. Oracle Label Security has been independently evaluated under the international common criteria and complies with government and commercial requirements for highly secure products.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Oracle Label Security
June, 2020