Understanding and Using HRMS Security in Oracle HRMS

Product: Oracle Human Resources **Minimum Version:**11.5.9

Abstract

Understanding and Using HRMS Security in Oracle HRMS

Document History

Author : Steve Cooper
Create Date : 04-OCT-2006
Last Update Date : 18-JUN-2008
Expiration Date :
Other Information :

Table of Contents

- **f) Security List Maintenance errors**

1. Overview

The purpose of this paper is to introduce and describe the key components of HRMS Security, to provide a technical analysis to enable a better understanding of the processes involved, and to give pointers as to why HRMS Security might not be working as desired. For a more detailed examination of how to set up Security Rules for your enterprise, please refer to the manual Oracle HRMS Configuring, Reporting and System Administration Guide.

a) Introduction

Users of Oracle HRMS access the system via a responsibility that is linked to a security group and a security profile. In the Standard HRMS Security model, when a business group is created a View All security profile is created ,and a security group of 0 (Standard) is automatically assigned. When security groups are enabled, a new security group gets created for each business group, and the association of a security group to a security profile is determined by the business group.

```
Example Querys using Standard Security Group

select security_group_id,
       security_group_name
from fnd_security_groups_vl
where security_group_id=0;




select name,
       business_group_id
from per_business_groups
where security_group_id=0
```

HR Users accessing the system via forms can only view data from one business group at a time,so before any security rules have been set up, HR data is already being restricted by business group. However, the "HR:Cross Business Group" profile option does allow certain fields to be used accross business groups when set. For example, Supervisor.

Managers accessing system using Self Service HR can, if required, see direct reports accross business groups (see Global Security Profiles).

HRMS Security allows you to further restrict access to data based on criteria you define in a security profile.

b) Security Profile

The Security profile is the means by which you determine what users of the system have access to what data. It determines which type of person's records are available. For instance, Applicants,Employees,Contingent Workers or Contacts.

You then determine which work structures or other criteria you want to use to restrict access. For example, a particular HR Adminstrator may only be given access to employees in organizations within a specific region, and only a senior Payroll clerk would be allowed access to employees in the Director's payroll.

The criteria you can use to identify these records are

Internal Organizations and Organization Hierarchies
Positions and Position Hierarchies
Payrolls
Supervisors and Supervisor Hierarchies
Custom restrictions
Assignments

The security profile will be discussed in more detail in the next section.

c) Security List Maintenance

Oracle HRMS enforces it's security rules by using secure views which call a security function (see Technical Evaluation) that works out access based on whether the security profile is dynamic or uses static lists. The static lists of people,organizations,payrolls,and positions are indexed against each security profile. They are maintained by a concurrent process called Security List Maintenance which is usually run overnight to ensure that any changes during the day that would affect the availablity of a person's record i.e. organization, is reflected in all secure responsibilities the following day.

Please note if security profile is dynamic and not static, Security List Maintenance need not be run. Dynamic or user-based profiles are Supervisor, user-based Organization and Position security, custom security using the 'Restrict the people visible to each user using this profile' option, or Assignment Level Security.

d) Security Models

There are two Security Models. Standard HRMS Security and Security Groups.

In essence this just amounts to how the security profile that you have defined is made available to the end user who will be using it.

Standard HRMS security is the traditional method. You Define a security profile, and you define a responsibility for use by application users. The two are linked by assigning the profile option,HR:Security Profile with the value of the relevant security profile, to the responsibility. It's a one to one relationship. To have access to other security profiles, you would need to create a new responsibility.

Security Groups on the other hand offer a means whereby you can reuse a responsibility and assign it to different security profiles in different business groups if required. You no longer use the HR:Security Profile profile option, as access to the security profile is granted by the form, Assign Security Profile. When you log on to the system you will see the same responsibility name but paired against different security groups (security profile and business group).

To enable security groups you set the profile option Enable Security Groups to Yes, and run the concurrent process Enable Multiple Security Groups. This will create a pair of records for each existing responsibilty. One associated with the Standard security group which is the Setup Business Group by default, and one with the defined business group. It is recommended to end date the responsibilty associated with the Standard business group to cut down on the list of responsibilities available to the user. However, it should be understood that those users using the Security Groups model who wish to update Global Lookup codes, must do it using the Standard security group.

An important consideration also is that once Security Groups have been enabled, you cannot return to the Standard HRMS Security model.

The profile option Enable Security Groups should be set at Application level as Non HRMS applications do not support multiple security groups. Shared HR always uses Standard Security.

The type of enterprises that would benefit from security groups would be multi-nationals, and service centres using multiple business groups and security profiles.

e) Reporting Users

The Reporting user is an often misunderstood aspect of HRMS Security. The purpose is to allow read-only access to the HR database by reporting tools like sqlplus and discoverer, but still using the secure views. To do this it is necessary to create an alternative oracle id to APPS which is what the standard Oracle Applications eBusiness Suite uses. You then need to create the security profile and associate the new reporting oracle user to it. Once that has been done you run the Generate Secure User process which Grants the HR_REPORTING_USER role to the REPORTING_ORACLE_USERNAME specified in the security profile. The HR_REPORTING_USER role already has select or read only permissions to all the HR objects.

f) Financials and Manufacturing

Certain Financial and Manufacturing business views are restricted by Operating Unit. They make use of the function HR_SECURITY.SHOW_BIS_RECORD, and in order to secure by operating unit, users are required to

a) Create a security profile with the security types

Secure Organizations by Single Operating Unit or
Secure Organizations by Operating Unit and inventory organizations.

b) set profile option MO:Security Profile

Security List Maintenance need not be run for profiles created using these two security types as they are dynamic. Security List Maintenance will not include them in the LOV as the ORG_SECURITY_MODE is OU and OU_INV respectively and excluded.

In Procurement Intelligence, a security profile should be set up using an Organization Hierarchy of Operating Units and, being static based, requires Security List Maintenance to be run.

See the Oracle® E-Business Suite Multiple Organizations Implementation Guide for information about setting up security profiles in Financials and Manufacturing.

See also Note 316829.1.

In Oracle Assets, users can set up Security by Book by having an organization hierarchy of Asset Organizations, defining a security profile with an entry point into the hierarchy,Running Security List Maintenance, and setting the FA:Security Profile on the responsibility with restricted access.

2. The Security Profile

The determining factors of what data is allowed to be accessed by a User/Responsibility are defined in the Security profile.

You decide what person types are available to the profile, whether individual assignments are restricted, and what work structures or other criteria to use to evaluate accessibility.

Person Types

On the Security Profile, you decide on each of the following person types whether to View All of them, to View None of them, or to have them Restricted according to the criteria laid out in the profile:

Employees
Contingent Workers
Applicants
Contacts
Candidates

Exceptions are that 'None' option is not available for Contacts, and 'Restricted' is not available for Candidates.

You can use any of the following criteria to restrict accessibility to data, or a combination of each.

a) Organization Security

You can either use an Organization Hierarchy to determine access, or you can specify a list of organizations to whom the user has access.

For the **List** method, simply select the Security type,'Secure Organizations by organization hierarchy and/or organization list' option. Then select each of the Organizations in the Oragnization Name field you want the profile to have access to. The include checkbox is automatically checked.

For the **Hierarchy** method, you select the Security type,'Secure Organizations by organization hierarchy and/or organization list' as before. Then you choose your Organization Hierarchy. The next step is to determine at which entry point into the hierarchy , access starts. This can either be by specifying the Top Organization, or allowing the top organization to be decided by the assignment of the user who is accessing the profile. You can also include organizations not in the hierarchy in the Organization Name field, or exclude organizations in the hierarchy. The business group can also be excluded, as can the top organization if required.

b) Position Security

Position security uses a Position Hierachy, and the entry point to determine where access starts can be based on the specified Top Position, or it can be taken from the assignment of the user who is accessing the profile. Top Position can be excluded if required.

c) Payroll Security

If restriction by payroll is required, the main thing to consider is the efficiency of the definition. For instance, if access to most payrolls are required, uncheck View All Payrolls and uncheck Include check box, then specify payrolls to be excluded.

To give access to a small number, uncheck View All Payrolls and check Include check box, then specify payrolls to be included.

d) Supervisor Security

This type of security profile is based on a Supervisor Hierarchy which by default is built up dynamically when the user logs on.

It can be Person based in that the user/manager has access to **ALL** the assignments of a person who reports to him, and those that report to his subordinate. The Primary Assignments Only checkbox is unchecked by default.

It can also be Assignment based, which would be used in conjunction with Assignment-Level Security.(see below). In this case the user/manager can only access the **specific** assignment that reports to him and the direct report of this assignment.

Supervisor security can cause an overhead when logging on to the system. Options for improving performance would be to restrict the number of Hierarchy Levels to go down or using a Static List which would create the supervisor hierarchy when Security List Maintenance is run (see Static Lists)

Remember that the user/manager is identified as an employee in the Define User form in the System Administrator.

iRecruitment uses supervisor hierarchies to control recruiter and manager access to vacancy information. You can set up a supervisor-based profile which restricts managers and recruiters to viewing only those vacancies that are managed by people reporting in to them.

e) Miscellaneous Security

Accessibility to records depends on the User Name used to log in, if this is a user based security profile. In other words , if this is a Supervisor Security profile, or if the entry point into the hierarchy of an Organization or Position based profile is determined by the assignment of the user logging in.

However,this can be bypassed, and the profile can always use the same user, no matter who logs in, by specifying the name of the user on the Miscellaneous tab.

Use the Exclude User check box to deny access to the user's own records, or the records of the Named User if specified. Option not available in SSHR.

f) Custom Security

Users can write their own code to restrict access in the Custom Security tab. You can choose to 'Restrict the People visible to the profile' which uses Security List Maintenance to store the data in a static list, or 'Restrict the people visible to each user using this profile' which is user-based security and evaluates access when the user signs on.

The user writes a 'where' clause fragment which is verified, and incorporated into the following select statement to work out accessibility:

```
select 1
from per_all_assignments_f ASSIGNMENT,
     per_all_people_f PERSON,
     per_person_type_usages_f PERSON_TYPE
where ASSIGNMENT.assignment_id = :asg_id
and :effective_date between ASSIGNMENT.effective_start_date
                        and ASSIGNMENT.effective_end_date
and PERSON.person_id = ASSIGNMENT.person_id
and :effective_date between PERSON.effective_start_date
                        and PERSON.effective_end_date
and PERSON.person_id = PERSON_TYPE.person_id
and :effective_date between PERSON_TYPE.effective_start_date
                        and PERSON_TYPE.effective_end_date
and (CUSTOM CODE GOES HERE)
```

A typical piece of custom code might look like this

```
ASSIGNMENT.location_id in (select LOC.location_id
from hr_locations_all LOC
where LOC.location_code
in ('London','Paris'))
```

However be sure to force character strings to upper case as custom restricted text is not case sensitive currently. see Note 965961.1.

The above custom code should therefore be rewritten as

```
ASSIGNMENT.location_id in (select LOC.location_id
from hr_locations_all LOC
where UPPER(LOC.location_code) IN (UPPER('London'),UPPER('Paris')))
```

Please note also that there is an issue using the PERSON_TYPE alias in the custom code which results in the following error

```
APP-PER-289835:  An SQL error was found in your custom restriction.
The error is `ORA-904: `PERSON_TYPE.PERSON_TYPE_ID:Invalid identifier.
Correct the error before continuing
```

For more information see bug 9622337

g) Static Lists/User-Based Security

Security Profiles which determine availability based on the user such as Supervisor Security, user-based Organization and Position security or custom security using the 'Restrict the people visible to each user using this profile' option, are evaluated at the point of logging in, which as mentioned previously can lead to performance overheads on some systems. Using Static lists in conjunction with these profiles can eliminate that overhead. You can specify the relevant users on the Static List tab, and the permissions will be stored when the Security List Maintenance program is run not when logging on.

Prior to R12 there is a limitation to user-based security, in that it doesn't allow access to ex-employees with a Final Process Date. From R12.1 there is a profile option called HR: Ex-Employee Security Profile. Set the Profile to Yes to include Ex-Employees, Ex-Applicants, and Ex-Contingent Workers ,or No to retain original functionality. Doesn't apply to Supervisor Security. See Bug 5612905 (NOT available as a one-off)

h) Assignment Level Security

Traditionally, accessibility to data in Oracle HRMS through security profiles was person based. So if a person had multiple assignments the profile only had to have access to one assignment to allow access to all.

This was not restrictive enough, and from Oracle HRMS Family Pack H a new feature was introduced to allow restriction based on individual assignment. There is a checkbox called Restict on Individual Assignment on the security profile definition.

This invoked Assignment Level Security in SSHR but only in 3 forms in the Professional User Interface (PUI) in Oracle HRMS Family Pack H, Oracle HRMS Family Pack I, and Oracle HRMS Family Pack J. The forms were

```
PERWSHRG (Combined Person / Assignment)
PERWSEMA (Fastpath Assignment)
PERWSQHM (People Management)
```

and had to have a parameter added to their function definition in System Administrator. The parameter was SECURE_ON_INDIVIDUAL_ASG='YES'.

From Oracle HRMS Family Pack K, this parameter has been removed and the list of PUI forms that support assignment-level security has been extended.

As with User-Based security, however, restricting by assignment is worked out dynamically which has the limitation of not giving access to ex-employees with a Final Process Date. see above.

i) Global Security Profiles

It is possible to setup security profiles whereby employees can be accessed accross different business groups. This may be for a variety of reasons:

```
1) Non HRMS users who do not want data to be restricted by Business Group
   when they define Global Security profiles
2) In Self Service HRMS, where Managers using Supervisor hierarchy have
access
   to direct reports accross business groups.
3) In R12 Professional HR, People Management can now be used with a Global
   Security profile. If a Global Security Profile is linked to the
responsibility
   users can choose the business group on the Find screen to query cross
business
   groups. Records can be updated and secondary assignments created, however
new
   employees are created in the default business group set by the HR:Business
Group
   profile option or in Assign Security Profiles form depending if Standard
security
   or security groups are used. All other forms accessed using the
responsibility
```

use the Global Security profile too, but are limited to using the default business group.

It may also be a simple device to consolidate security profiles. A profile could include organizations accross business groups, but when attached to one business group in the Professional User interface, only the employees in that business group are visible.

If access accross business groups is required, a Global Security Profile must be created in Navigate ->Security -> Global Security Profile. Payroll and Position security is not available in Global Security profiles. Neither is Reporting User access. The Global Security Profile is identifiable as having a null business_group_id on the table PER_SECURITY_PROFILES.

3. Technical Evaluation

Access to data via Oracle HRMS is provided by views. The majority of these views restrict the data available to a user/responsibilty by joining with cached data which holds information about what people can be viewed by what security profile. The cached data is either loaded from the static lists or dynamically at logon time.

a) Static Lists

The lists are

PER_PERSON_LIST

PER_ASSIGNMENT_LIST (not currently in use)

PER_ORGANIZATION_LIST

PER_POSITION_LIST

PAY_PAYROLL_LIST

These lists are cleared and refreshed by the Security List Maintenance program. As Assignment_level_security is currently only dynamic, the static list PER_ASSIGNMENT_LIST is not yet used.

b) Secure Views

The Secure Views,for example PER_PEOPLE_F, include a call to the function HR_SECURITY.SHOW_PERSON which returns TRUE if the person record is visible to this security profile, otherwise FALSE. Other views which are secure may not directly call this function, but query secure views like PER_PEOPLE_F.

HR_SECURITY.SHOW_PERSON determines whether the security profile is static or dynamic, and evaluates access accordingly.

As previously mentioned , for Financial and Manufacturing users, many business views such as PABG_CUSTOMERS and POBG_STD_PURCHASE_ORDERS call the function HR_SECURITY.SHOW_BIS_RECORD which secures data according to the security profile referenced by MO:Security Profile profile option.

Here is a script that can be used to run queries on HR secure views in sqlplus.

Firstly get the values of the ids in angle brackets by doing Help -> Diagnostics - Examine in a form after logging in using the responsibility for the secure user.

```
e.g.  BLOCK - $PROFILES$
      FIELD - USER_ID
      VALUE -
```

then substitute in the values.

The script counts the records available to this user/responsibility in the secure views and base tables for person and assignment.

```
SET SERVEROUT ON

DECLARE
 l_per_all  NUMBER := 0;
 l_per_sec NUMBER := 0;
 l_asg_all NUMBER := 0;
 l_asg_sec NUMBER := 0;

BEGIN

 fnd_global.apps_initialize(, , , );

 SELECT count(*)
 INTO l_asg_all
 FROM per_all_assignments_f
 WHERE business_group_id = ;

SELECT count(*)
 INTO l_per_all
 FROM per_all_people_f
 WHERE business_group_id = ;

 SELECT count(*)
 INTO l_per_sec
 FROM per_people_f;

 SELECT count(*)
 INTO l_asg_sec
 FROM per_assignments_f;

 dbms_output.put_line('Per all: ' || to_char(l_per_all));
 dbms_output.put_line('Per sec: ' || to_char(l_per_sec));
 dbms_output.put_line('Asg all: ' || to_char(l_asg_all));
 dbms_output.put_line('Asg sec: ' || to_char(l_asg_sec));

END;
/
```

4. Troubleshooting Problems

a) Check Setup

Most security problems are usually to do with the fact that the security profile in question is not working as expected in that it is giving access to the wrong data.

The following check list can help to identify why this might be.

1. Run Security Diagnostics to verify security setup

Introduced in Family Pack K, and a good place to start your investigation. Using the Oracle Diagnostics functionality, you can run Security Diagnostics to evaluate and debug your security setup for Oracle HRMS. The tests check that your security setup is correct for your requirements and identify common issues and problem areas.

```
The tests produce the following report types:

 o Summary   - Summary of all security profiles used in your setup

 o Detail    - Detailed information on the security profile assigned to a
given

               responsibility.

 o Usage     - Usage information on the security profile assigned to a given
               responsibility, for example, which responsibilities use the
               security profile.

 o Access    - List of organizations, payrolls, positions, and optionally,
               person assignments, a named user can access using a given
               responsibility.

 o Exception - List of security profiles defined in the system whose set up
is

               treated as an exception in the HRMS Security model.
```

See: Metalink Note #305644.1 (Human Resources (HRMS): Security Profile Setup Diagnostic Test)

2. Is the responsibility accessing the correct security profile?

Establish the security_profile_id of the Security profile in question by running the following in sqlplus:

```
    set linesize 180
    select security_profile_id,
           substr(security_profile_name,1,40)
      from per_security_profiles;
```

then logon to the application using your secure responsibility, and navigate to Enter and Maintain People (PUI only). Do Help -> Diagnostics -> Examine and enter the following:

```
    BLOCK - $PROFILES$
    FIELD - PER_SECURITY_PROFILE_ID
    VALUE -
```

Check whether the id displayed against VALUE is the one that relates to your security profile.

If this is not the case then if Standard HRMS Security, you have not set the profile option HR:Security Profile at the correct level or, if Security Groups are enabled you have not used the Assign Security Profile form to link the security profile to your user/responsibility.

3. Check that the security profile is set up correctly?

For static list security, the acid test is whether the person to whom access is expected appears on the table PER_PERSON_LIST.

```
      select person_id
        from per_person_list
       where security_profile_id=&security_profile_id
```

If no row, then either the program Security List Maintenance hasn't been run, or the rules for this profile do not allow access to this person.

If they do appear then the record should be visible.

For Supervisor security, access is determined by the user logging in and which assignments report into him.

Does the user who is logging on have an employee attached?

select employee_id from fnd_user where user_name = &user

Please note that the supervisor set up can yield different results depending on the rules. i.e. whether person based or assignment based and whether Restrict on individual assignment check box is set. See the Oracle HRMS Configuring, Reporting and System Administration Guide for further explanation.

For user-based, Organization and position security, the entry point into the hierarchies is determined by the primary assignment of the user logging in.

For custom security, the sql that gives access can be validated by appending the custom sql to the stem code specified in section 1).

4. Check the data

In particular check the assignment data of an identified person to see if the criteria used for determining the security rule is valid for this person.

5. Check patch level

The latest HRMS Security RUP is 4643909 which requires Family Pack F or above.

b) HRMS Security and Datetrack

Access to people's records via HRMS Security is established

a) For Static lists, by the defined criteria on the effective date on which Security List Maintenance is run.
b) For user-based security, by the defined criteria at SYSDATE.

Accessibility is **NOT** re-evaluated when datetracking.

This can have different effects when users datetrack forward or back depending on the security profile and the person's employment history.

When a security profile is defined, accessibility to person types can be Restricted, All or None.

Accessibility is governed

a) by having a row on the secure person list if the person has a person_type that is Restricted on the security profile.
b) By not having a row on the secure person list if the person only has a person_type that is All on the Security profile. Eligibility is taken for granted in this case.

This can lead to different results if there have been multiple person type changes. For example

Security Profile - Person Type Test
View Employees - Restricted
View Contingent Workers - All
Restricted to all people in the Human Resources organization.

Scenario 1

Person is an Employee in the Sales organization, and not visible to this profile. On 1st May, the organization of the employee is changed to Human Resources and he is now visible because when the secure list was calculated either at sysdate or effective date of the Security List Maintenance program, he was an Employee, and in the Human Resources organization, and a row was inserted onto the secure person list according to case a) above.

Datetracking to before the 1st May when the person was in Sales does not remove accessibility even though the profile excludes him as accessibilty is **NOT** re-evaluated.

Scenario 2

Person is an Employee in the Human Resources organization, visible to this profile. He is terminated and becomes an ex-employee on 30th April. On 1st June he becomes a Contingent Worker in the Human Resources organization and is visible by this profile.

Datetracking to before 30th April does not retain accessibility however, because when the secure list was last calculated either at sysdate or the effective date of the Security List Maintenance program, he was not an Employee, and a row wasn't inserted on the secure person list according to case b) above ,as the profile is View All on Contingent Workers. Even though the profile includes him at the date, when he was an employee, accessibilty is **NOT** re-evaluated, so he is not visible.

c) Prior to 12.06 User-Based or dynamic security gives access to Active assignments only

Ex-employees (if beyond Final Process Date), Ex-applicant, and Ex-Contingent workers are not visible because they won't have an active assignment on sysdate. In order to see this type of person, you will need to define a security profile using static security and run Security List Maintenance for Current and Terminated people.

Contacts are also not visible using dynamic security.

The same applies to assignment-level-security which currently works out assignment accessibilty dynamically only.

To recap, user-based or dynamic security includes

Supervisor Security
User-based Organization and Position security where top organization is determined by assignment of user logging on.
Custom security using the 'Restrict the people visible to each user using this profile' option.
Assignment-level-security.

Remember also that if a security profile has been created with no restrictions at all. i.e. is View All. This will also be evaluated dynamically. Consider the case where a user has created a profile to view all employees and ex-employees only. This will be evaluated dynamically and filter out ex-employees which is not what the user requires. To resolve that they would need to force the profile to be static. To do this they could enter restriction under the Custom tab. Choose "Restrict the People visible to this profile" and enter 1=1 in where clause. Then run Security List Maintenance

N.B. From R12.06 the option to include the EX person types in user-based or dynamic security profiles is provided by setting the profile option, HR Ex-Employee Security Profile' to Yes. From R12.1 the profile was renamed to HR: Access Non-Current Employee Data. Doesn't apply to Supervisor Security, and Contacts are still excluded. Set to No to retain original functionality of restricting to Active assignments only. <> (Not available as a one-off patch).

d) Performance Issues

The most common places to see performance degradation would be at logon time when a dynamic security profile is being processed, or whilst running Security List Maintenance to maintain the static lists.

Please take note of the following patches:

4643909 - Latest HRMS Security RUP (Family Pack F or above)
4444325 - Security List Maintenance performance issue (FP J)
5214715 - Security List Maintenance performance issue (FP K)
4932555 - Dynamic security causing performance problem (FP K)

n.b. all the above are included in FP K RUP1 (5055050)

Another area to check is possible poorly performing custom sql in the custom tab of the security profile definition. Never use secure views in custom code. Also beware of causing full-table scans on assignment.

Think about how you use and schedule Security List Maintenance. It can be run multi-threaded now. Calling the PERSLM process many times for single profiles continually hits the person and assignment tables. Running multi-threaded accesses the person and assignment tables less times, and gives better performance in global implementations.

Also consider separating SLM runs for current and terminated employees.

e) Generate Secure User errors

The problem with this program is that on 99% of occasions, the user shouldn't be running it at all. It would be better named as Generate Secure Reporting User, as it simply grants the HR_REPORTING_USER role to an Oracle user other than APPS which is used for reporting purposes only.

There is no need to run this program if you are just defining normal security profiles to restrict user access to data using the standard Oracle HRMS Application forms and html interfaces.

The following sql can be run to check whether any reporting oracle users have been used on security profiles.

```
select security_profile_id,
       security_profile_name,
       reporting_oracle_username
from per_security_profiles
where reporting_oracle_username IS NOT NULL;
```

If no reporting users, **DO NOT** run this program.

f) Security List Maintenance errors

If the Security List Maintenance program has errored out, then on occasion it may be necessary to further debug it by running PYUPIP. The following steps should be taken to get a PYUPIP trace based on FP K Patch level. Change parameters as appropriate. If on a different patching level, it may be necessary to add or remove some parameters:

```
1. Login to the SQLPLUS
2. Set serveroutput on
3. spool pyupip.out
4. Execute the following

BEGIN
hr_utility.set_trace_options ('TRACE_DEST:DBMS_OUTPUT');
hr_utility.trace_on;
pay_pyucslis_pkg.generate_lists(
p_effective_date => trunc(sysdate)
,p_generation_scope => 'ALL_PROFILES'
,p_business_group_id => NULL
,p_security_profile_id => NULL
,p_security_profile_name => NULL
,p_who_to_process => 'ALL' -- Current and Terminated people
,p_user_id => NULL
,p_static_user_processing => 'ALL_STATIC'
);
hr_utility.trace_off;
Exception
when others then
dbms_output.put_line(sqlerrm);
hr_utility.trace_off;
END;

5. spool off
```