

LaGov HCM

Security

Administration

User Guide

TABLE OF CONTENTS

| | | |
|-------------|--|----------|
| I. | INTRODUCTION | 1 |
| A. | Objectives | 1 |
| B. | Overview of LAGOV HCM Security | 1 |
| C. | Duties & Responsibilities | 2 |
| II. | GENERAL INSTRUCTIONS | 3 |
| A. | Accessing LAGOV HCM | 3 |
| | LAGOV HCM Userids | 3 |
| B. | LAGOV Passwords and the LEO System..... | 3 |
| | Password Restrictions | 3 |
| | Changing Passwords | 4 |
| | Password Problems | 4 |
| C. | Contacting the LAGOV HCM Security Help Desk..... | 4 |
| III. | ROLES..... | 6 |
| A. | Paid Processor..... | 6 |
| | Basic Employee Administration | 6 |
| | Enhanced Employee Administration | 6 |
| | Organizational Management..... | 6 |
| | Employee Administration Time Management..... | 7 |
| | Retro Authorization | 7 |
| | Time Administrator | 7 |
| B. | Non-Paid Processor | 7 |
| | Organizational Management..... | 7 |
| | Employee Administration | 7 |
| C. | Special Authorizations..... | 8 |
| | Inquiry Access | 8 |
| | Agency Fiscal..... | 8 |
| | DPS Reporting | 8 |
| | Personnel Development | 8 |
| | DOTD roles | 8 |
| | Training Coordinator | 8 |

- LSO\QUAL Reporting..... 8
- D. Control Agency Roles..... 8
- E. Restrictions 8

- IV. Online LaGov Security Application..... 10**
 - A. Online LaGov Security Application Access 10
 - B. Sign-on Instructions for the Online LaGov Security Application 11
 - C. Online LAGOV Security Application Logon Screen 12
 - D. LAGOV HCM Security Main Menu 13
 - E. General Instructions for Using LAGOV HCM Security Forms 13
 - F. LAGOV HCM Security Forms 15
 - LAGOV HCM Request for Position Security - ISF048 15
 - LAGOV HCM Request for Control Agency Position Security - ISF050 17

- V. SECURITY REPORTS..... 18**

- VI. DELIMITATION OF LAGOV HCM SECURITY 20**
 - A. Delimitation of Position Security 20
 - B. Delimitation of Userids..... 20

I. INTRODUCTION

This is a guide for LAGOV HCM Security. Every new agency LAGOV HCM Security Administrator and Alternate must request access to LAGOV HCM before using the Online LaGov Security application.

An Online LaGov Security application section is included in the user's guide to instruct HCM Security Administrators and Alternates on how to submit forms through the Internet. We recommend that you look at the actual forms in the Online LaGov Security application as you read the section on forms.

A. Objectives

The objectives of this guide are to show the HR Security Administrator and Alternate how:

- LAGOV HCM security is structured.
- To complete and submit appropriate security forms through the Online LaGov Security application.
- To find LAGOV security related information via online system and reports.

B. Overview of LAGOV HCM Security

- LAGOV HCM security is centrally maintained by the OIS HCM Security Administrator. The OIS HCM Security Administrator may be contacted by calling the LAGOV Help Desk.
- All LAGOV security forms should be submitted through the Online LaGov Security application.
- The Agency HCM Security Administrator will be the contact person at the agency through which all security related forms and/or questions should first be routed. The Alternate should be the next contact person at the agency and will serve as a backup. The Alternate will also receive correspondence from LaGov staff.
- Security questions or changes should be routed to either the Agency HCM Security Administrator or Alternate. They will then forward any questions or changes to the OIS HCM Security Administrator.
- Department Undersecretary or Agency Appointing Authority (only where no Undersecretary exists) must submit a form to designate or change the HR Security Administrator or Alternate. This form, **ISF061**, is available on the OIS web site under Forms, Miscellaneous and should be forwarded to OIS.
- New LAGOV HCM security records will be activated by OIS each night during the security job run.
These jobs run Monday – Friday of each week except Payroll Monday. Changes made to LAGOV HCM security on Payroll Monday will not take effect until Wednesday of payroll week. Notification is sent to the Agency HCM Security Administrators and Alternates after requests are processed.

C. Duties & Responsibilities

- The Agency HCM Security Administrator or Alternate should review all forms for accuracy before submitting them through the Online LaGov Security application to OIS.
- All forms must be printed before being submitted through the Online LaGov Security application. The Agency HCM Security Administrator and Alternate must **sign all forms** as indicated. The Agency HCM Security Administrator and Alternate will be responsible for keeping a hard copy of the form at their agency.
- The Agency HCM Security Administrator and Alternate should maintain a file with signed copies of all forms submitted to OIS for future reference and audit purposes.
- When a security request has been completed by OIS, the Agency HCM Security Administrator and Alternate will receive electronic notification. However, the userid may not be ready for use until the security update program runs, even if the position relationship records appear complete.
- Audit warning:** The auditors expect access to be limited to a business need only. They also may consider certain permission combinations to be incompatible.
- When an employee is promoted or moves to a different position, but should continue to have the same security access, the security permissions attached to the previous position must be assigned to the new position. HCM security does not transfer to the new position with the userid.
- It is the agency's responsibility to submit a **Remove** request when a position no longer needs permissions attached. This would be whenever the holder of the position will not have assigned duties to work in LAGOV HCM. The auditors expect this to be done in a timely manner.

II. GENERAL INSTRUCTIONS

A. Accessing LAGOV HCM

LAGOV HCM Userids

- New LAGOV HCM userids are created by a nightly batch process. When an employee is added into the system a userid is automatically created in LAGOV HCM for that employee. This process runs on Monday through Friday night during non-payroll weeks and Tuesday through Friday of payroll-week. At the same time the userid will be assigned the permissions, which are attached to the position for which the employee is a holder. New employees in non-paid agencies also have userids created through the same process.
- For new users, it is the responsibility of the agency to look up the employee's new personnel number and give them their userid. The personnel number can be found through transaction PA20 Display Master Data. The userid will consist of the personnel number preceded by a "P" followed by sufficient zeros to make a nine-character userid.

Ex. New employee number is 211234.
The employee userid would be P00211234

The initial password for a userid is setup by the employee in the LEO system under password maintenance. It is the responsibility of the agency to instruct new employees on how to use LEO password maintenance. For users who have LAGOV HCM security access, the password set up in LEO will be the password used for all LAGOV HCM functions.

B. LAGOV Passwords and the LEO System

- A password can only do its job of protecting you and your ID if you handle it properly and that means keeping your password strictly confidential; no sharing.
- Avoid writing your password down and leaving it where others might see it.
- Avoid using easy to guess passwords such as the names of your children, significant other, pets, favorite sports teams or religious references.
- Since the ID is assigned to you, your name is associated with all the activity your ID performs. The following list of password rules was formulated to help protect your good name and the data you depend on.
- Passwords are case sensitive.

Password Restrictions

- Passwords must be selected within the guidelines listed:
 - must be eight characters to forty characters
 - must contain at least one number and one letter
(cannot be all alphabetic or all numeric)
 - cannot be your first name or last name
 - cannot begin with abbreviation of any month
 - cannot begin with sequential series (e.g. 1234, abcd, etc.)
 - cannot begin with pass
 - cannot be the same as the last five passwords used

- The security of a user's password ultimately rests with the user. Never save it when prompted. Avoid using obvious choices. Users should also avoid recycling a group of passwords over and over again. Most importantly, however, never share a password with a co-worker. A user's userid is his or her unique identification; any activity performed using a userid can be traced to the person to whom it was assigned.
- A userid can never be reassigned to a different person. System users who experience a name change should see a change in the name displayed on the LAGOV HCM user menu once their personal data record has been updated with the new name and the nightly security job stream has been run. This should only be done in the case of a legal name change. The name on the user's personal menu will also be changed to match the employee name in LAGOV HCM on the personal data record.

Changing Passwords

- Your password is good for 90 days and may be changed as desired through LEO. After 90 days, the system will prompt you to replace your expired password. You may change expired passwords in LaGov HCM or at any time access LEO password maintenance to change your password. If the new password does not conform to the rules listed above, the system will display an error message and you must try again. Once your password is changed, it will be available to access LAGOV HCM and LEO.

Password Problems

- After three incorrect attempts to enter the correct password, your userid will be suspended. The unsuccessful attempts need not be one right after the other. The counter for password violations continues tracking attempts until a successful sign on takes place.
- If your ID is suspended or you have forgotten your password in LAGOV HCM, you must use password maintenance in LEO. LEO can be found at <https://leo.doa.louisiana.gov>. If you get a message that your LEO account is disabled in password maintenance or you cannot answer your ssn or date of birth, then you must contact the LEO help desk. The help desk will ask you for your name, userid and work phone number. The help desk representative will ask you to give your date of birth and the last 4 digits of your SSN. (This information is used to confirm your identity.) If you can match this information, they will remove the lock, reset your personal questions and instruct you to set up a new password in LEO password maintenance. It is then the user's responsibility to use LEO to set up a new, confidential password at the earliest possible opportunity. The LAGOV HCM system will not allow the user to sign on until he or she selects a new password. Help desk representatives will not assign passwords to a userid. It is the user's responsibility to maintain their own password for LAGOV HCM and LEO. When the user selects a new password in LEO password maintenance, the account is unlocked. Employees will always use the same userid and password to log into both LAGOV HCM and LEO.

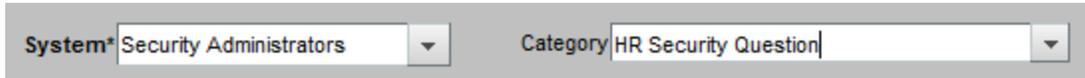
C. Contacting the LAGOV HCM Security Help Desk

The LAGOV HCM Security Help Desk can be contacted either by phone or by submitting an online OIS Help Desk Web Ticket. The Help Desk should be contacted for questions involving security access, assignment and maintenance of security roles, filling out and submitting security requests, the availability of specific transactions and their relationship to security roles, establishing access for security

administrators and other questions concerning LAGOV HCM security

The LAGOV HCM Security Help Desk is available to assist users by phone from 7:30 am to 4:30 pm. The help desk can be reached at 225-342-2677, Option 1, 3.

The LAGOV HCM Security Help Desk can also be reached using the OIS Help Desk Web Ticket. A link to this ticket is on the OIS home page at <http://www.doa.la.gov/ois/index.htm>. Once the ticket is accessed, select **ISIS- Security Administrators** as the System and **HR Security Question** as the Category. The options should look like those shown below.



System* Security Administrators Category HR Security Question

Please provide a brief description of the problem or question in the Problem Details section of the ticket. The OIS Help Desk Web Ticket will be received by the LAGOV HCM Security Help Desk via email and you will be contacted during normal Help Desk business hours.

III. ROLES

In LAGOV HCM, permissions are grouped together into logical sets called roles. Roles are based upon job functions. In order to request the correct security for a user it is necessary to understand what roles are available and what type of job duties will be performed by an employee in each role. All security granted will have reporting and inquiry access corresponding to the permissions given.

A. Paid Processor

Basic Employee Administration

This role includes:

- All personnel actions except transfer, including the hiring action, separation action, organizational assignments and position characteristic changes;

- Benefits processing actions including enrollment, overview, termination and confirmation;

- Merit administration including processing, review and release of appropriate merit increases through compensation management, manual merit processing and maintenance of employee ratings;

- Authorization for Payroll Simulation, Time Evaluation, Quota Overview and Absence Quotas.

Enhanced Employee Administration

This role includes all permissions in the Basic Employee Administration role plus:

- Transfer actions;

- Leave payouts and adjustment of annual/sick leave accruals and balances;

- Authorization of off-cycle checks;

- Retro Authorization involving entry of all changes with an effective date prior to the current pay period.

Organizational Management

This role includes:

- Maintenance of the agency org structure including creation and maintenance of org units, positions and their relationships;

- Maintenance of Organizational Assignments.

Employee Administration Time Management

This role has all the permissions of the Time Administrator role but on the personnel area level, plus:

Maintenance of Planned Working Time, Time Evaluation and Quota Overview;

Retro Authorization involving entry of changes that have an effective date prior to the current pay period.

Retro Authorization

This role is authorization to enter all changes that have an effective date prior to the current pay period. It cannot be the only role requested but can be added to Basic Employee Administration or Organizational Management.

Time Administrator

This role allows entry of attendance and absences, plus certain premium, shift differential and on-call pay. Permissions are set at the time administrator number level.

B. Non-Paid Processor**Organizational Management**

This role allows:

Maintenance of the agency org structure including creation and maintenance of org units, positions and their relationships;

Maintenance of Organizational Assignments;

Retro Authorization involving entry of changes that have an effective date prior to the current pay period.

Employee Administration

This role allows:

All Personnel Actions;

Maintenance of HR Master Data;

Retro Authorization involving entry of changes that have an effective date prior to the current pay period.

C. Special Authorizations

Inquiry Access

This role allows a user to view records within the assigned agency number or numbers only. Reporting is also allowed with this level of permissions with statewide access to Organizational Management data. This role is included in all EA processor roles and should not be requested separately.

Agency Fiscal

This role allows agency Fiscal Staff reporting access to their agency(s) financial data within LAGOV HCM.

DPS Reporting

This role allows for a special reporting category for the Department of Public Safety. Other agencies may not request this role.

Personnel Development

This role allows tracking of FEMA course completion information and skills qualifications obtained upon completion of other training courses. It may only be requested by DHH.

DOTD roles

These roles may only be selected by DOTD.

Training Coordinator

Provides information and runs reports on employee course enrollment, qualifications, etc. Approves and schedules courses for employees who do not self-enroll through LSO.

LSO\QUAL Reporting

Runs reports on employee qualifications and training activities.

D. Control Agency Roles

The ISF050 shows the Roles that have been created specifically for Control agencies. These agencies should only select those roles specific to their agency. For a description of the various control agency roles, please see the instructions for form ISF050.

E. Restrictions

Some combinations of permissions are incompatible and should not be requested together. If you request an EA Processor role you will be allowed to update records in the system, therefore it would be impossible

for an Inquiry Access role to be assigned because you cannot be allowed to update records at the same time you are limited to only display records. These roles are contradictory so the request would be rejected.

All of the permissions included in the Basic Employee Administration role are also included in the Enhanced Employee Administration role, so both roles cannot be selected.

The Employee Administrator Time Management role allows users to update records in PA61 for their entire personnel area; therefore it is unnecessary to request timekeeper permissions in that personnel area for someone who has this role. If the two are requested together the form will be rejected.

Agency Fiscal permissions should be limited to no more than three per Personnel Area in the case where it is the only permission requested for a particular position. There is no recommended number for those positions that have other permissions assigned. If the position already has the Inquiry role or EA level maintenance, Agency Fiscal authorization should not be requested since it is already included in these roles.

Permissions specific to an agency may not be requested by other agencies.

IV. Online LaGov Security Application

- The purpose of the Online LaGov Security application is to make it possible to complete all security requests online.
- Agency security staff must print an original copy of each document, obtain signatures, and then electronically submit the request to OIS. It is the responsibility of the agency security staff to keep signed copies of all security requests on file. Once requests are processed, Agency HCM Security Administrators or Alternates will receive a message confirming that their security request has been completed. The confirmation will go to the email address entered on the form.

Note: *Electronic forms must be printed before being submitted. The Online LaGov Security application will not provide an opportunity to print a form after it has been submitted.*

A. Online LaGov Security Application Access

- All Online LaGov Security application users will be assigned a unique userid and password. Userids and passwords are case sensitive. The userid should be typed in all **CAPS** and the password is all **lower case**.
- Your userid and password **must not be shared** since standard LAGOV security protocol must continue to be followed.
- When the HCM Security Administrator's and Alternate's responsibilities change within an agency, OIS should be notified immediately so that the appropriate userids can be added, changed or inactivated. These changes can be submitted with the approval of the Department Undersecretary or Agency Appointing Authority (only where no Undersecretary exists) on form ISF061. This form is found on the OIS web site under LaGov ERP Support, Forms.
- Please address any questions concerning Online LaGov Security application userids or passwords to the LAGOV Security Help Desk.

B. Sign-on Instructions for the Online LaGov Security Application

- Click on the Internet Explorer icon:
- Type or click on the following Web address:

<http://www.doa.louisiana.gov/ois/LaGov/LaGovSec.htm>

The link will take you to the LaGov ERP Security page. Click on the Online LAGOV Security application link.

The screenshot shows the Louisiana.gov website with the following content:

- Navigation Menu (Left):** OIS HOME, ISIS SYSTEMS, ISIS SYSTEMS SUPPORT, LAGOVERP, LAGOVERP SUPPORT, SYSTEM LOGINS, HELP DESK, MEMOS, OTHER USEFUL LINKS.
- Director Information (Bottom Left):**

DIRECTOR
Martha O'Hara
 Tel: (225) 342-0900
 Fax: (225) 342-0902
 Email: Martha.O'hara@la.gov
 Mailing Address:
 P.O. Box 94095
 Baton Rouge, LA 70804-9095
 Physical Address:
 Claiborne Building
- Breadcrumb Trail (Top):** Louisiana.gov > Division of Administration > Office of Information Services
- Page Title:** LaGov ERP Security
- Main Content:**

Each agency must designate both a primary LaGov HCM security administrator and an alternate LaGov HCM security administrator for the following areas of LaGov:

 - Human Capital Management (HR)
 - Includes Learning Solution (LSO)
 - Travel

Use form [ISF061](#) to designate primary and alternate security administrators. Both the primary and alternate security administrators will be assigned a userid and password and will have the authority to submit security request forms electronically to the OIS LaGov Security Administrator.

Security guides can be found in LEO under **My Work>Publications**.

Security administrators can access the LaGov Security Application by clicking

[Online LaGov Security application](#)

Agency staff can view who their agency security administrators are in LEO under **My Work>Agency Contact Information**.

DOTD may also submit requests for other LaGov modules including:

 - Financial
 - Project Systems
 - Logistics – Plant Maintenance/Linear Assets
 - eProcurement and Inventory/Warehouse Management

These requests require completion of the appropriate security form (see forms in table below).

If you use a shortcut or favorite to access the LAGOV ERP Security page and when you click on the link you receive a message that the page cannot be displayed, go to the OIS home page and click on the LaGov ERP Support/Security link in the menu on the right.

C. Online LAGOV Security Application Logon Screen

- Enter your user name.
- Enter your password.
- Leave the Authentication field blank.
- Click Login.
- If you receive the message 'Invalid password or authentication string for an existing user', please check that your password is correct and is being entered in lower case. If the message is displayed again, please contact the LAGOV Security help desk.
- If you receive the message 'User has no access permission to the form isishrsecurity', please contact the LAGOV Security help desk.

BMC Remedy Action Request System

A screenshot of the BMC Remedy Action Request System logon screen. The background is a blue gradient with a large white play button icon. On the left, there is a small image of a tunnel with a car. On the right, the text "Please log in." is displayed above three input fields labeled "User Name", "Password", and "Authentication". Below the input fields are two buttons: "Log In" and "Clear".

Please log in.

User Name

Password

Authentication

Log In Clear

D. LAGOV HCM Security Main Menu

- Click on the form you would like to access.

LaGov Security

LaGov Security Forms

NOTE: Only the forms that you are authorized to submit are displayed below.

ISF048 - Human Capital Management

ISF050 - Human Capital Management Control Agencies

Exit

E. General Instructions for Using LAGOV HCM Security Forms

- **Push Buttons** Left click on the push button you wish to select.

| | |
|---------------|---|
| Print | Prints the LAGOV Security Form. |
| Submit | Send LAGOV Security Request form to OIS Security Administrator. |
| Clear | Set all the fields on the form to blank. |
| Close | Takes you to the sign on screen. |
| Menu | Takes you back to the main menu. |
- **General Fields**

| | |
|-----------------|---|
| Comments | Enter comments you wish to make. |
| Required Fields | All fields with the titles in bold letters are required fields. |
| Optional Fields | All optional fields are in non-bold letters. |
| System Fields | All fields generated by the system are italicized. |
- Agencies that are not Control agencies (those that have access to statewide data) should use the ISF048.

- Control agencies should normally use form **ISF050** instead of **ISF048**. An exception is when a Control agency employee does not perform a control function involving other agencies (such as a clerical employee who is a timekeeper).
- If the print warning pop-up does not appear for new users, a pop-up blocker is on. All pop-up blockers must be turned off for the system to work properly.
- A link to instructions for completing the form is found at the bottom of each form.
- The error message 'REQUIRED FIELD (WITHOUT A DEFAULT) NOT SPECIFIED: *field name*' will be received when a required entry has not been provided. All missing information must be entered before the form can be successfully submitted.
- The Agency HCM Security Administrator is required to keep signed copies of all LAGOV Security Request forms for audit purposes.
- After the information is entered on the form, the HCM Security Administrator or Alternate must print and then submit the LAGOV Security Request Form. Forms cannot be printed after they have been submitted.
- All forms must be submitted electronically. A pop-up will appear stating that the form has been successfully submitted.
- All printed forms must be signed with the appropriate signatures and kept on file by the agency.
- The expected turnaround time for security requests is two days.
- Security is activated by the nightly security update job stream. Once a security request is returned as completed, the security will be available after the update runs, normally the next business day.
- The security job stream **does not run** on the Monday night of a payroll week due to payroll processing. Security that has a start date that is the Monday of a payroll week will not be available until Wednesday.

F. LAGOV HCM Security Forms

LAGOV HCM Request for Position Security - ISF048

ISF048
Rev. 12/2011

LaGov HCM

Request for Security

Position # OR External Person # Personnel Area

Personnel Area Access

Limit security within an agency? Yes No
 If yes, list the 3 digit personnel admin. group code.

Action

New Revised
 Remove Temp Auth

Start Date

End Date

LaGov HCM AUTHORIZATIONS

Select the processing authority to be granted for the position number listed above. All previous authorizations for the position list will be replaced by the selections indicated herein.

Note: Both BASIC EA and ENHANCED EA cannot be selected.

Paid Agency EA Processor

BASIC EA
 ENHANCED EA
 EA TIME ADM
 ORG MGMT
 RETRO CALC

Special Authorizations

INQUIRY ACCESS DOTD BUSINESS MANAGER
 AGENCY FISCAL TRAINING COORDINATOR
 DPS/WLF REPORTING LSO TRNG REPORTS ONLY

Non-Paid Agency EA Processor

ORG MGMT
 EMPLOYEE ADMINISTRATION

Time Group-

| Pers Area | TA Grp |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> |
| <input type="text"/> |
| <input type="text"/> |
| <input type="text"/> |

Authorization to Assign Security

I authorize the access indicated on this form. I understand that should this access no longer be required within LaGov HCM that I am to submit this form to the Division of Administration OIS Security Administrator within one working day.

LaGov HCM Security Administrator or Alt. SA Phone SA Email

SA/Alternate Comments

Form Instructions: <http://www.doa.louisiana.gov/OIS/Service/Forms/Instructions/isf048->

- Position number** must always be included.
- If the Action is...
 - New** Position security will be added.
 - Revise** Position security will be replaced with the requested permissions.
 - Remove** Removes all LAGOV HCM security when a position no longer requires it.
- Temporary Authorizations** .All permissions listed on the form will be the position security for the time period designated.
- Inquiry Access permissions should not be requested with any maintenance permissions.
- Basic EA and Enhanced EA cannot both be requested.
- Timekeeper permissions cannot be requested with EA Time Management permissions.
(EA Time Management allows time entry for the entire personnel area).
- If some security access is being removed from a position but other security relationships will remain active, a form must be submitted with Revised selected within the action section. All security listed on the form will remain with the position.
- If all security is being removed, a form must be submitted with Remove selected within the Action section. The LAGOV HCM AUTHORIZATIONS section must be blank. No security roles can be selected.
- When Agency Fiscal access is granted to positions that do not have other HR permissions, each personnel area is limited to 3 Fiscal-only IDs. All the functions of Agency Fiscal are included in Inquiry Access.
- DPS/WLF Reporting is limited to Department of Public Safety and Wildlife and Fisheries personnel only.
- DOTD roles may not be requested by any other department.
- When an agency needs additional Timekeeper Groups in LAGOV HCM, submit the request to the LAGOV Security help desk indicating both the personnel area and how many new Timekeeper Groups are required. When LAGOV Security staff receives the request they will respond with the numbers of available, unused Timekeeper groups within the Personnel Area. Agency Security Admin or Alternate may then begin using any of those groups or may request the creation of new groups, if needed. New groups can be requested on Form ISF048 with an additional comment stating the reason and number of new groups needed. When LaGov Security Staff receive a request to assign a new Timekeeper group(s) to a position, they will initiate the creation of the new group(s). LAGOV Security staff will notify the HR Security Administrator and Alternate when the request is complete and assign the position security if requested on the ISF048.

Note: These types of request take longer to process due to the additional steps.

LAGOV HCM Request for Control Agency Position Security - ISF050

ISF050 **LaGov HCM - Control Agencies**

Request for Position Security

Position # **Personnel Area**

Personnel Area Access -List all agency numbers to access.

Action
 New Revised Remove Temp Auth

Start Date **End Date**

LaGov HCM AUTHORIZATIONS

Select the processing authority to be granted for the position number listed above. All previous authorizations for the position listed will be replaced by the selections indicated herein.

| Civil Service Roles | OIS Roles | OSUP Roles | Control Agency Inquiry Roles |
|--|--|---|--|
| <input type="radio"/> Inquiry | <input type="radio"/> Security Administrator | <input type="radio"/> Financial Inquiry | <input type="radio"/> Lasers Inquiry |
| <input type="radio"/> Job Processor | <input type="radio"/> Payment Proposal | <input type="radio"/> BFA Processor | <input type="radio"/> CPTP Inquiry |
| <input type="radio"/> State Police Comm | <input type="radio"/> Sys Admin Security LTC | <input type="radio"/> GA Processor | <input type="radio"/> OPB/Legislative Fiscal Inquiry |
| <input type="radio"/> Legacy System Update | <input type="radio"/> Job Monitor | <input type="radio"/> WTA Processor | <input type="radio"/> OGB Inquiry |
| <input type="radio"/> Compliance Inquiry | <input type="radio"/> Portal Administrator | | <input type="radio"/> OSRAP Financial Inquiry |
| <input type="radio"/> Training Administrator | <input type="radio"/> Workflow Administrator | | <input type="radio"/> TRSL Inquiry |
| <input type="radio"/> LSO Instructor | <input type="radio"/> Travel User Support | | <input type="radio"/> Field Auditor/IG |
| | <input type="radio"/> Travel Technical Support | | <input type="radio"/> LSPR Inquiry |
| | <input type="radio"/> TDH User Support | | |
| | <input type="radio"/> LSO Administrator | | |
| | <input type="radio"/> Instructor | | |

Authorization to Assign Position Security

I authorize the position named above to have the access indicated on this form. I understand that should this position no longer require access within LaGov HCM that I am to submit this form to the Division of Administration OIS Security Administrator within one working day.

LaGov HCM Security Administrator or Alt. **SA Phone** **SA Email**

SA/Alternate Comments

Form Instructions: <http://www.doa.louisiana.gov/OIS/Service/Forms/Instructions/isf050->

- Position number** must always be included.
- If the Action is...
- New**..... Position security will be added.
- Revise**..... Position security will be replaced with the requested permissions.
- Remove**..... Removes all LAGOV HCM security when a position no longer requires it.
- Temporary Authorizations** .. All permissions listed on the form will be the position security for the time period designated.

Roles on this form are limited to particular control agencies. The form lists roles specific to Civil Service, Office of State Uniform Payroll (OSUP), and Office of Information Services (OIS). Other agencies should not request these roles.

Several agency specific "Inquiry Only" roles are listed on the form under the heading "Control Agency Inquiry Roles". These have been created especially to allow inquiry access for Lasers, CPTP, OPB, OSRAP, TRSL, Inspector General and OGB. Other agencies should not request these roles.

V. SECURITY REPORTS

The following reports can be viewed/printed in LAGOV HCM by entering the transaction in the transaction bar in the upper left hand corner of the SAP screen.

- These reports should periodically be reviewed by the LAGOV HCM Security Administrator and/or Alternate. They are some of the same reports that the auditors will use.
- ZS06 –Position Security Report**

Position Security Report

Date Parameter

Today
 Other Date 08/21/2008

Selection Criteria

| | | | | |
|-------------------------|--|----|--|---|
| Company Code | | to | | → |
| Personnel area | | to | | → |
| Position | | to | | → |
| Personnel number | | to | | → |
| Include Selection Roles | | to | | → |
| Exclude Selection Roles | | to | | → |

Output positions, no roles
 Show Roles on User IDs

This report can generate a list by Personnel Area of positions which have active LAGOV HCM security on the date the report is generated. The report lists the holders of the positions and their effective dates as well as the security validity dates. It also provides the last logon date for that user, the printer assigned to that user, the organizational unit and the organizational unit text.

If a position has access to security in several personnel areas, the report will only list the position in the personnel area which owns the position. LAGOV HCM Security Administrators should therefore run this report for all personnel areas in which they can assign security. This report should be reviewed periodically to verify the security assigned to positions so that corrections can be made before an audit occurs.

The report has the flexibility to exclude or include security roles or report security for a specific position, personnel number or security role. ZS06 can be run to output only a list of positions and holders for audit counts or a list of positions with the attached security roles if more detail is required.

Personnel areas must be entered as four digits such as 0326. Personnel numbers should be entered as the numeric value only.

An alternate date can be entered by selecting Other Date.

If no security is assigned to the position, the message 'No Data Found for Selection Criteria' will be returned.

When the ZS06 is run for a position or personnel number, all security roles are listed including technical roles that are assigned automatically. These technical permissions are added to a security request so that the LAGOV HCM system will work properly for the security role(s) assigned. A security role is also added to allow access to SAP through the LEO portal. These technical roles are not listed on the ISF048 or the ISF050 Remedy ticket and may vary according to the security role(s) selected. They do not need to be requested.

For those security roles that are assigned through the ISF048 or ISF050, the Role Name column shows the role as it is listed on the Remedy ticket. Use this column to identify the security currently assigned to the position or personnel number.

Samples of the ZS06 security report are shown below for an HR Analyst profile and Time Administrator profile.

HR Analyst Security Profile

| Security Role | Role name |
|----------------------|--|
| ZHR_OM_0165 | Org Management Role for Agency 0165 (PAID) |
| ZS_USER | General Authorizations given to all R/3 users |
| ZHR_EATA_0165 | EA Time Administrator Role for Agency 0165 |
| ZHR_ENH_0165 | Enhanced EA Processor for Agency 0165 |
| ZHR_INQSTATEWIDE | Statewide Inquiry Role |
| ZHR_REPT_0165 | Paid Rept role for EAs & Inquiry Only users in Agency 0165 |
| Z_PORTAL_LEOMSS_0165 | LEO Portal Role with MSS Permissions to Agency 0165 |
| ZLSO_TRAINCOORD_0165 | LSO Training Coordinator Role for Personnel Area 0165 |

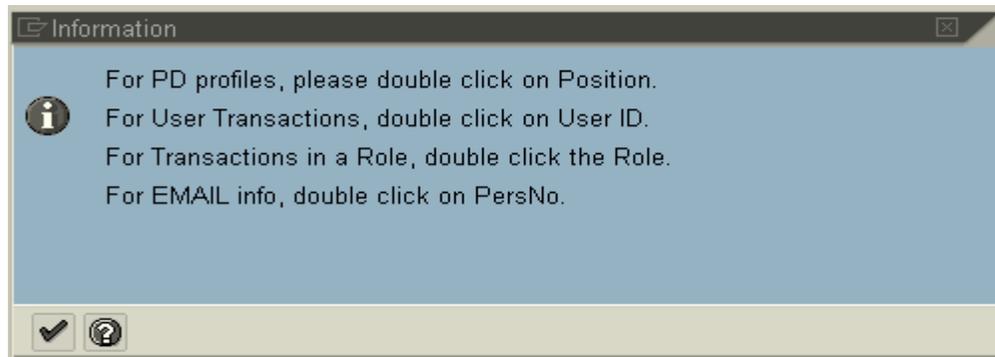
This security profile has Org Mgt, EA Time Administrator, Enhanced EA and Training Coordinator as assigned roles.

Time Administrator Profile

| Security Role | Role name |
|-----------------|---|
| ZHR_TA_0370_055 | Time Admin for personnel area 0370 ID 055 |
| ZS_USER | General Authorizations given to all R/3 users |
| Z_PORTAL_PRDGUI | Enables portal users to access the WEBGUI |
| ZHR_TA_0370_055 | Time Admin for personnel area 0370 ID 055 |
| ZS_USER | General Authorizations given to all R/3 users |

This profile has two Time Groups assigned. The ID is the number of the Time Group.

The ZS06 report can provide even more detailed information concerning security assigned to the position when the **Show Roles on User IDs** box is checked before the report is run. Once the report has been generated, all columns shown in brown can be used to access additional information.



VI. DELIMITATION OF LAGOV HCM SECURITY

A. Delimitation of Position Security

There are two ways that this can occur.

1. If a position no longer requires permissions in LAGOV HCM, the Agency LaGov HCM Security Administrator or Alternate must send in form ISF048 to remove the security.
2. When an employee leaves a position (through reassignment or separation) and no longer has a valid holder relationship to the position, the position security is delimited from the userid. Programs do this during the nightly security job run.

Vacant positions can still have security relationships attached. When a holder is assigned to a position, the existing security relationships automatically become attached to the holder's userid when the nightly security update program runs. If the new holder will perform the same job duties and require the same security permissions, no action is necessary. However, if a position no longer requires HCM security access, the HCM Security Administrator/Alternate should remove all security relationships by submitting a form ISF048 even if the position is currently vacant.

Security Administrators\Alternates are responsible for properly maintaining LAGOV HCM position security.

At the discretion of the LAGOV HCM staff, audits may be run to remove position security due to the limited number of licenses available in SAP. For example, an audit could list Time Administrators who have not entered time during the previous twelve months and have not logged on to the HCM system in the past three months. It is advisable for all HCM users to log on to SAP at least once every three months.

B. Delimitation of Userids

Occurs as a result of the Separation action.