Introduction
The following document is intended for Agency Security Liaisons for creating and managing CO-1092 Security Requests. The CO-1092 Security Request page will only display User IDs for employees a Security Liaison has access to in Core-CT; this is determined by the Liaison’s Primary Permission list (Row Security) in the HRMS system. Department Row Level Security in Core-CT determines the employees a User will have access to in the various HRMS modules or EPM. This is further defined by the Row Security field on the General Tab on the User Profile page. Each User will have a unique Permission List value in this field that is generated by the system. The Row Level Security Permission List will comprise of the User’s Employee ID preceded by ‘DP’.

In the example below, ‘DP025037’ is the Row Level Security Permission List for Employee ID 025037 (User ID ‘CTSECLIAISON’):

Navigation: Core-CT HRMS > Peopletools > Security > User Profiles > User Profiles
Department ID BOR85500 is assigned to the ‘DP025037’ Row Security Permission List; therefore, this user will only have access to employees in Department BOR85500:

Once a CO-1092 Security Request has been processed, the CO-1092 Search Page can be used to see pending, denied and completed requests. Security Liaisons will be unable to select User IDs on the CO-1092 form if the Agency Acronym in Department Description of the User Profile is for an agency they do not have access to. Note: For employees that have transferred into your agency, please contact the Core-CT security team at corect.security@ct.gov to have the agency acronym updated; after which point the User ID will be made available.

**CO-1092 Security Request – New Request**


2. The Security Liaison will click on the **Add New** tab.
CO-1092 Security Request

Enter any information you have and click Search. Leave fields blank for a list of all values.

3. The **Transaction Number** will not be editable, but will auto-generate when the CO-1092 Security Request is saved.

4. The **Transaction Date** will not be editable, but will default to the current date and has no impact on when the security request will be completed and processed.

**CO-1092 Security Request**

- **Transaction Number:** 0
- **Transaction Date:** 04/16/2013
- **User ID:** 

5. **User ID** field is required to know which employee needs to obtain new roles, delete existing roles, or update other security items such as Row Level security, Time and Labor groups or Business Units. If you know the User
ID you can enter it in the field, otherwise, you can search by using the magnifying glass icon to the right of the field. This will open a search dialog that allows you to search using Description and/or User ID.

**Note:** The lookup will allow you to see all User Profiles in the system; however, you are only allowed to select User ID’s for which you have access to create CO-1092 Security Requests.

6. When the **User ID** is selected click on the Add button.

7. The following fields will be automatically populated when the **User ID** is selected: **Employee ID, Name, Email ID, and Telephone** on the CO-1092 Security Approval Page.
   a. **Employee ID** is retrieved from the employee User Profile table and does not have any impact on how the request is approved. This field is informational only.
   b. **Name** is retrieved from the employee names table and does not have any impact on how the request is approved. This field is informational only.
   c. **Email ID** field is retrieved from the employee User Profile table and does not have any impact on how the request is approved. This field is informational only.
   d. **Telephone** field is retrieved from the employee phone numbers table and does not have any impact on how the request is approved. This field is informational only.
8. The Manager User ID field is required to route the Security Request to the proper approving manager. Once a Security Request has been submitted, the manager will receive a request to approve the transaction. The Manager User ID field will only allow selection of Managers who have the CT_CO1092_APPRV_MGR role assigned to their user profile.

9. The following fields will be automatically populated when the Manager User ID is selected:
   a. Manager ID is retrieved from the managers User Profile table and does not have any impact on how the request is approved. This field is informational only.
   b. Manager Name is retrieved from the employee names table and does not have any impact on how the request is approved. This field is informational only.
   c. Manager E-mail address is retrieved from the User Profile table and does not have any impact on how the request is approved. This field is informational only.

10. Row Security section of the page help define the following:
    a. **Edit Departments (HRMS only)** - Effective Tuesday, November 8, 2016, maintenance of Department Row Level Group security was removed from the on-line CO1092 Security Requests form and central processing for this by Core-CT Security will no longer be necessary. Please refer to the ‘Department Row Level and Time & Labor (TL) Group Security Training for Agencies – Addendum to the CO1092 Training for Liaisons’ job aid on how to setup Row Security in Core-CT: [http://www.core-ct.state.ct.us/security/pdf/Row_Level_TL_SEC_Trng.pdf](http://www.core-ct.state.ct.us/security/pdf/Row_Level_TL_SEC_Trng.pdf)
b. **Edit TL Groups (HRMS only)** - Effective Tuesday, November 8, 2016, maintenance of TL Group security was removed from the on-line CO1092 Security Requests form and central processing for this by Core-CT Security will no longer be necessary. Please refer to the ‘Department Row Level and Time & Labor (TL) Group Security Training for Agencies – Addendum to the CO1092 Training for Liaisons’ job aid on how to setup Row Security in Core-CT: [http://www.core-ct.state.ct.us/security/pdf/Row_Level_TL_SEC_Trng.pdf](http://www.core-ct.state.ct.us/security/pdf/Row_Level_TL_SEC_Trng.pdf)

a. **Business Units (Financials CO1092 only)** – If the Row Level Security permission list is not known, the Business Units page will allow the Liaison to specify which Business Units a User ID will have access to. If information is entered, the Core-CT Security team will determine the best option.

b. **Origins (Financials CO1092 only)** – If Origins need to be added or removed to/from a user’s profile, the changes will be made on the Financial Appendix page ([http://www.core-ct.state.ct.us/security/xls/fin_appdx.xls](http://www.core-ct.state.ct.us/security/xls/fin_appdx.xls)). After the financial appendix page is completed, the Security Liaison will attach it to the online Security Request via the Comments Tab.

**Note:** When adding an Origin, please remember to add the role under the Security Roles section of the online CO-1092 even if the user already has the role.
c. **Additional Comments** – The Comments page can be used to enter ad hoc comments among between Security Liaisons and multiple approvers. Please limit this space to text entry only. If PDF or other types of documents need to be referenced, they can be attached. Also, if additional supporting documentation is needed for justifying the need for conflicting roles, the Comments page is also where a Liaison would include any pertinent comments and attachments such as any agency internal audit procedures required by OSC or DAS.

11. **Security Roles (Add/Delete)** section is used to specify the roles that should be added or deleted for the User Profile selected. Use the + and – buttons on the far right of the grid to add or remove rows of data.
12. The following rules apply for Security Roles:
   a. If Roles are being **Added** and
      i. If the User Profile does not have a Security Role assigned that is being selected, the Description will be: “This is a Valid Role.”
      ii. If the User Profiles already has a Security Role being selected, the Description will be: “The User Profile already has this Security Role.”
      iii. If the User Profile already has a Security Role such as CT AGY HR SPECIALIST, and a Security Role being added conflicts with the existing role because of segregation of duties, the Description will be: “This role conflicts with existing role: CT AGY HR SPECIALIST.”
      iv. If one or more Security Roles being added conflict with Segregation of Duties, the Description will be: “Segregation of Duties exception.”
   b. If Roles are being **Deleted** and
      i. If the User Profile has the role being deleted, the Description will be blank.
      ii. If the User Profile does not have the role being deleted, the Description will be blank.
13. When the roles have been added to the Security Roles (Add/Delete) grid you can Save the form and the following will happen:
   a. The transaction number will be auto-generated and saved for the transaction you have created. Use this transaction number to track the request. You can always come back to it and make changes if the Request has not been submitted for approval. Once the CO-1092 Security Request has been submitted for approval, you can no longer make changes.
14. When the form is ready to be submitted for approval. Save the form and then click the **Submit** button.