

PS 8052.02 MILLENNIUM AUTHORIZATIONS



Program Statement

OPI: FPI
NUMBER: 8052.02
DATE: 9/25/2003
SUBJECT: Millennium
Authorizations

1. **PURPOSE AND SCOPE.** To establish standards for creating and maintaining access authorizations in **Millennium**.

2. **SUMMARY OF CHANGES.** These changes were made to this PS:

- ◆ The User Administrator must assign the account of an employee leaving UNICOR to the "Expired" user group;
- ◆ A System Change Request process is delineated when it is necessary for a user to have additional transaction authorizations that are not allowed in his or her user group; and
- ◆ Branch Chiefs are responsible for identifying Critical Combinations using the System Change Request process to the ERP Branch.

3. **PROGRAM OBJECTIVES.** The expected results of this program are:

a. Roles and responsibilities for the development, maintenance, and assignment of user authorizations in **Millennium** will be clearly defined.

b. Security of information in **Millennium** will be maintained by proper internal controls over user permissions to conduct transactions.

4. **DIRECTIVE AFFECTED**

a. **Directive Rescinded**

PS 8052.01 Millennium Authorizations (10/19/01)

b. **Directive Referenced**

PS 1237.11 Information Security Programs (10/24/97)

5. **STANDARDS REFERENCED.** None

6. **RESPONSIBILITIES.** This section defines the roles and responsibilities of the following positions within UNICOR:

a. **SAP Security Administrator.** This position, within the Management Information Systems Branch (MISB), is responsible for monitoring **Millennium** security and developing the required procedures.

b. **User Administrator.** This position is responsible for creating and maintaining user accounts at field sites. One user administrator must be appointed for each UNICOR operation site and, typically, is the System Administrator or designated backup.

c. **Authorization Administrator.** This position, located within MISB, is responsible for creating activity groups used to grant access for specific functions in **Millennium**.

7. **MILLENNIUM SYSTEM LOGON ID.** All staff, contractors, vendors, and inmates granted access to UNICOR's **Millennium** system will be issued only one Logon ID per person.

8. **ASSIGNMENT OF MILLENNIUM ACTIVITY GROUPS.** It is through the User Administrators' assignment of activity groups that individual users are granted authorization to perform specific transactions. Each activity group contains transactions which include definitions of functions authorized for the user to accomplish.

- ◆ The SAP System has been configured with role-based activity groups. Activity groups are modified and additional ones developed and maintained by the Authorization Administrator.
- ◆ Staff are assigned automatically to the Activity Group "All_staff" and inmates assigned to the Activity Group "All_inmates."

a. Role based activity groups are named and assembled based on the functions required for the specific job performance.

Example: The activity group "Plant-manager" contains the transactions required to perform a Factory Manager's duties and responsibilities.

b. Field site User Administrators assign activity groups to users based on the duties assigned to each position. Activity groups, which are assigned either as a collateral duty or on a temporary basis, are to be documented in an electronic file and granted only for the time period for which management authorizes them to be functioning in the special capacity.

- ◆ Documentation of these temporary authorizations will be maintained for one year.

c. The User Administrator will secure the account when a user leaves UNICOR by locking the account and assigning it to the "Expired" user group.

For users who are transferring to another UNICOR location, the User Administrator will modify the account to view only and assign it to the "Expired" user group.

- ◆ The User Administrator at the new location will make the appropriate assignments for usage at the new location for transferring users.

9. **REQUESTING CHANGES TO EXISTING AUTHORIZATIONS.** When an individual user needs authorization to perform a transaction that his or her assigned activity group(s) does not permit, he or she should contact the User Administrator to attempt resolution first.

- ◆ The User Administrator may be able to grant the authorization needed by assigning an additional existing activity group to the user.

System Change Request. If the authorization cannot be provided through the assignment of existing activity groups, a system modification request must be initiated. To initiate a system modification, a system change request (SCR) must be submitted through the appropriate Business Unit Manager to the Chief, Enterprise Resource Planning Branch (ERP) on a Systems Change Request form that can be found at www.fpi.gov.

The ERP branch will determine the SCR's feasibility and facilitate the creation of the authorization if it is found to be feasible.

10. **CRITICAL COMBINATIONS.** Critical combinations are defined as transactions that must be assigned to separate users to comply with current policy, or as a matter of security and/or internal control management.

Branch Chiefs are responsible for identifying critical combinations that impact their areas of responsibility and reporting them to the ERP Branch via the SCR process.

- ◆ Upon completing their review and testing, the ERP Branch will forward all critical combinations to the System Security Administrator.

The System Security Administrator must:

- ◆ maintain documentation of critical combinations;
- ◆ load them into the system; and
- ◆ generate a report periodically to ensure there are no violations.

The Financial Management Branch must review the critical combinations report listing all known combinations at least annually to ensure compliance with current policy. Any violations detected will be referred immediately to the proper User Administrator for correction with a copy to the Associate Warden/Superintendent of Industries or Branch Chief.

The User Administrator will review the critical combinations report when assigning and/or making changes to an individual's activity group.

/s/
Harley G. Lappin
Director