March 13, 2011

SUPERVISION AND REVIEW
USER ACCESS CONTROL & DATASET ACCESS REVIEW

OVERVIEW

These procedures apply to periodically reviewing individual's access level to the Office of Personnel Management's Sysplex environment. It gives direction to all mainframe Data Owners, Designated Security Officer/ Security Officer (DSO/SO), Supervisors, and those involved with determining access authorization for users of the OPM's mainframe applications.

PURPOSE

The purpose of this document is to establish procedures for the periodic access authorization, review, and revocation of an individual's access to mainframe applications, such as ARPS, DCCS, Control-D, etc. The procedures also describe the process for revoking access to these applications.

ASSUMPTIONS

The procedures below discuss the process where by a RACF Security Administrator, Supervisors and DSO/SO perform certain functions to review access control for users under their control.

DEFINITIONS

Authorized User – a person who has been authorized to access mainframe applications for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with OPM. The authorization granted is for a specific level of access to the RACF protected resources.

Resource Access Control Facility (RACF) -RACF is the security component of the z/OS operating system. RACF provides the tools to manage user access to critical resources. RACF protects resources by granting access only to authorized users of the protected resources. RACF retains information about users, resources, and access authorities in special structures called profiles in its database, and it refers to these profiles when deciding which users should be permitted access to protected system resources.

RACF Security Administrator – Data Center (DC) Security Team provide top-level access to the OPM Sysplex environment through the Resource Access Control Facility (RACF) security software. Three business entities comprise this

Sysplex environment – Administrative System (AS), Federal Investigative Services (FIS), and Center for Retirement and Benefits (RB). A formal approval procedure is established in this document and is followed to ensure the integrity of the OPM Sysplex (a.k.a. enterprise server) systems.

Designated Security Officers/Security officers – Are the contact persons for specific user groups or applications (depending on the business entity involved). These officers are responsible for approving the necessary access and updating any internal application security prior to forwarding the request to the DC Security Team.

Access Authorization Procedures – Access to mainframe applications will be granted based on legitimate business need as determined by the individual's supervisor, data owner and DSO/OS. The DC Security Team will grant access after receiving approval from the supervisors and DSO/SO.

User Access Review & Dataset Access Review Procedures - Access to mainframe applications will be reviewed periodically in accordance with the following procedures:

1. **Schedule for User Access Review**

- User access will be reviewed **quarterly** (after the initial review that began August 2007) by the supervisors and DSO/SO to reapprove all users and their access to the RACF protected resources. This review presumes that all access is explicitly denied unless re-authorized through this process.
- The data owners, supervisors and DSO/SO are required to verify that each account on the access list should remain active and the access permissions are current.
- The DSO/SO or supervisor(if no DSO) must sign, date, and return the
- Supervision and review access control form to DC Security Team within 15 business days distribution. If the supervisor or DSO/SO fails to return the list within 15 business days, then all account on the list will be suspended until the list is received.

Generation of Access Reports

To facilitate the review schedule listed above, the DC Security Team will generate a report of all Userids, which have access to the mainframe application systems under the scope of this document. This report will detail the level of access each user maintains. The report will be distributed to the supervisors and DSO/SO for review.

- Each DSO/SO or supervisor will review each account under his or her responsibility for appropriateness.

- An individual user must only have access to RACF resources necessary to perform his or her job responsibilities. All access beyond that which is required for the person's job function is considered unauthorized.
- If a the supervisor and/or DSO/SO determines that an inappropriate level of access is granted to an individual, are required to inform the DC Security Team to remove all the noted access.

Dataset Access Review

Annually, DC Security Team will generate a RACF cross- reference report. This report displays every explicit reference to the RACF Userid and Group in the RACF database. RACF cross-reference report will identify every dataset rule access list; facility class access list; CICS transaction access list and RACF Group connection for each Userid and Group.

This report is provided to each DSO asking that they review and verify that users and groups have the right access to RACF protected resources. This ensures that all access remain accurate and current.

DC Security Team will make any changes the DSO deems necessary and keep a record on file. In the event that the DSO doesn't discover any changes, the security administrator shall file the email as proof of the review.

Access Revocation Procedures

When an individual resigns, terminated, transfers, or for any reason no longer needs access to mainframe applications, the Userid and all access will be immediately removed.

1. **Notification From Management**

Supervisors or the DSO/SO must notify the DC Security Team indicating that a subordinate employee should no longer have access to the mainframe application(s). When the DC Security Team receives this notice, he/she will immediately remove the Userid and all access to the application(s).

2. **Notification From User**

Employees may send written notice to the DC Security Team stating that access to the application is no longer needed. The RACF administrator will remove access to RACF resources.

3. **Periodic Revocation of RACF Accounts**

On a weekly basis, the DC Security Team will compare RACF accounts to a file received from the Human Resources System to ensure that accounts are deactivated for terminated employees. If application access is involved, the employee's supervisor or DSO/SO will notify the appropriate administrator to deactivate the user's application accounts.

Employee Access Change Procedures

Keeping track of employee movement and separations is critical to maintaining an up-to-date security database. Changes in employee status that affects their system access requirements **must be reported by the DSO/SO or supervisor** to the security administrators as soon as the change is known.

Security administrators generate and review weekly reports showing which users have not accessed the system for between 90 for contractors and 1 year for federal employees.

Deleting Userid Guidelines:

Deletion of Userids will occur in the following situations:

- User is an OPM employee who becomes separated (separation, retired, etc) according to the Separation file provided weekly by OPM's personnel office (OHREEO).
- User is identified in the Interagency Transfer file provided weekly by OPM's personnel office (OHREEO) and who no longer requires access to Sysplex resources. If customer is moved to another program area within the agency, then they are contacted for requirements and must submit proper forms for approval to those resources.
- User is a contractor or ERC users whose Userid has not been active in the last 90 days.
- User is an OPM employee who has not accessed the system within 1 year.
- User completes exit form and turns into Help Desk, who notifies Data Center Group security administrators.
- Supervisor or DSO contacts security administrator(s) and request immediate deletion.
- COR contacts security administrators requesting removal of contractor Userids.
- User has repeated security violations, which raise concerns of intent to security administrators who may delete Userid until user's supervisor is notified.

Security administrators also rely on administrative reports to determine data access. In order to do this, security administrators require the following.

Notice of Reassignment or Detail

The security administrator receives notification when an employee changes offices or jobs. Upon notification of reassignment, the security administrator modifies the user's security profile and function group permissions as required. The inter-agency employee transfers report is run and disbursed to all DSOs/supervisors weekly. It is the **responsibility of the DSO/SO or supervisor** to immediately inform the security administrators of any changes that need to be made to the user's security profile. This report is produced after receiving the weekly report from OHREEO listing all inter-agency transfers.

Notice of Separation of Contracted Users

Notification of separation or reassignment is required for contractors as well as OPM employees. Each contracted group is required to report employee status every 30 days. This status includes separations of contracted employees on an OPM contract within the last 60 days. All current contracts or any new contracts will be modified to include this requirement.

If the status of the contract is not received every 30 days, an email will be issued to the Contract Project Manager giving a 5 working day extension for delivery of the status report. After that time, if no report is received, then all contractors under the specified contract will be suspended from access to the Sysplex until the report is received.