The Grants Gazette

Ohio EMA's Preparedness Grants Updates

August 2013 *Issue 19*

Compliance Tip of the Month

Commingling and Supplanting Overview

COMMINGLING

- Mixing or blending of funds so that expenditures cannot be identified to a particular grant, project, or indirect activity.
- Grantee records must identify the source and application of funds for federally sponsored activities.
- A separate account is established for each project.
- The financial system must provide for effective control over and accountability for all funds, property, and other assets.
- Recipients shall safe guard all such assets and assure they are used solely for authorized purposes.

SUPPLANTING

- To deliberately reduce State or local funds because of the existence of federal funds.
- Recipients shall not replace appropriated State or local funding with Federal grant funding.
- Grant funds should increase the overall amount of resources available.
- Recipients must ensure that the current overall level of funding to support objectives is not reduced because of federal funds.
- *For example*: Local funds are appropriated for purchase of an EMA base radio and Federal funds are awarded for that same purpose. The local agency replaces its funds for the base radio with Federal funds, thereby reducing the total local amount available for the original project.

Spotlight of the Month

Grants Computer Security Access

The first line of defense in computer system database accounts security is the user having authorized access. Proper password management is one of the most effective and necessary measures in restricting unauthorized access. To ensure that physical security and access to grant programs and data are appropriately controlled to prevent unauthorized use, recommend the following password security objectives be implemented:

- Access to systems shall be limited to authorized users and passwords will be assigned to user accounts by their immediate supervisor or database administrator per your agency policy.
- The protection of a password is the responsibility of the user. Users should safeguard and keep their passwords confidential. ***Equipment users must never share or give their password to anyone.*** Each user should have their own account with login information.
- When passwords are entered, users should make sure that no one is watching them key the password. Passwords should not be written on post-it notes attached to the workstations, office walls or in any way visible to other employees or visitors.
- Passwords should be removed from systems when the employee no longer reports to the organizational unit where he/she was originally assigned. User accounts should be deactivated by their immediate supervisor or database administrator per your agency policy.

Important Dates

- **BSIR due *August 30, 3013*.**
- **SHSP grant application due *September 16, 2013*.**
- **FY12 EMPG Supplemental requests due September 17, 2013.**

HSGP Grant Expenditures

As of August 30, 2013

Grant	Award	Expended	Remaining
FY 2011	$20,499,771	$11,173,335	$9,326,436
FY 2012	$6,224,189	$662,037	$5,562,152

For any questions or comments, please contact your Field Liaison.