TEXAS WORKFORCE COMMISSION
Workforce Development Letter

ID/No:	WD 13-19
Date:	June 5, 2019
Keyword:	AEL; Financial Reporting
Effective:	Immediately

To: Local Workforce Development Board Executive Directors
Adult Education and Literacy Grantees
Adult Education and Literacy Special Project Grantees
Other Agency Grantees
Commission Executive Offices
Integrated Service Area Managers

From: Courtney Arbour, Director, Workforce Development Division

Subject: **Online Security Verification Procedures for the Cash Draw and Expenditure Reporting System**

PURPOSE:

The purpose of this WD Letter is to provide Local Workforce Development Boards (Boards), Adult Education and Literacy (AEL) grantees, and other Texas Workforce Commission (TWC) grantees with new online security verification procedures for TWC's Cash Draw and Expenditure Reporting (CDER) system.

RESCISSIONS:

WD Letter 32-07

BACKGROUND:

In June 2019, TWC will begin using online procedures within the CDER system to perform annual security verifications of CDER system user permissions. Previously, TWC conducted CDER system security verifications entirely by e-mail. The new online procedures will replace the current e-mail process.

Boards and grantees use the CDER system to report obligations and expenditures, request and receive payments, and complete financial closeouts for TWC grant awards. The CDER system uses unique user passwords and permissions to control system access. One member of each Board's and grantee's staffs serves as the CDER system Security Administrator (Security Administrator) for that entity's CDER system users. Security Administrators control user permissions for certain CDER system functions and participate in TWC's CDER system security verifications.

TWC began conducting security verifications of Boards' CDER system user permissions in May 2007. TWC subsequently expanded CDER system use and security verifications

to grantees. Boards and grantees will both use the new online procedures to participate in TWC CDER system security verifications.

The new online procedures for TWC's CDER system security verifications involve Security Administrators' online review and certification of a CDER system Security Report. The Security Report identifies CDER system user access permissions for all the respective Board's or grantee's CDER system users. The report also includes two radio buttons: one to certify that the permissions listed on the report are appropriate, and one to notify TWC that one or more permissions require changes. When performing the system verifications, TWC staff will add each entity's Security Report to the CDER system and e-mail a notice to each Security Administrator. The security verification starts on the date that TWC e-mails the notice to the Security Administrator, unless the notice specifies a different start date.

Boards and grantees will have 15 calendar days from the start date of the TWC security verification for their Security Administrators to complete the following steps.

1. Review the Security Report in the CDER system.
2. Submit any needed CDER system user permission changes to TWC, await an e-mail notice from TWC that the Security Report has been updated with the changes (which may take up to two business days), and review the updated Security Report in the CDER system. Note: Submitting permission changes and awaiting TWC notice that the Security Report is updated for the noted changes does not "stop the clock" with respect to the 15-day deadline.
3. Certify the Security Report (or updated Security Report, if applicable) in the CDER system.

The Security Report is considered to have been certified by the Security Administrator after all CDER system user permission changes (if any) have been submitted to TWC, and the Security Administrator selects the certify option on the Security Report (or updated Security Report, if applicable) and then clicks "Submit" in the CDER system.

By certifying the Security Report, a Security Administrator certifies to TWC that:

- CDER system user permissions listed on the Security Report are necessary and appropriate for those users' roles; and
- adequate separation of duties or compensating controls exist to safeguard grant funds with respect to CDER system user permissions.

A Board or grantee that does not certify its Security Report by 11:59 p.m. on the 15th day of the TWC security verification will temporarily lose all CDER system cash draw permissions. The lockout will exist until the entity's Security Administrator certifies the Security Report.

Each Security Administrator will receive an e-mail from TWC at the end of TWC's security verification. TWC's CDER system will retain record of the online certification.

TWC's CDER system Security Verification training module provides detailed instructions for completing the CDER system security verification in the CDER system. The module is available on TWC's Cash Draw & Monthly Expenditure Report System web page at https://www.twc.texas.gov/agency/cash-draw-monthly-expenditure-report-system.

PROCEDURES:

No Local Flexibility (NLF): This rating indicates that Boards and grantees must comply with the federal and state laws, rules, policies, and required procedures set forth in this WD Letter and have no local flexibility in determining whether and/or how to comply. All information with an NLF rating is indicated by "must" or "shall."

Local Flexibility (LF): This rating indicates that Boards and grantees have local flexibility in determining whether and/or how to implement guidance or recommended practices set forth in this WD Letter. All information with an LF rating is indicated by "may" or "recommend."

TWC Annual CDER System Security Verification

NLF: Boards and grantees must certify the CDER system Security Reports within 15 calendar days of the start date of the TWC annual security verification, as described in this WD Letter.

Certification requires Boards' and grantees' Security Administrators to complete the following three steps:

1. Review the Security Report in the CDER system.
2. Submit any needed CDER system user permission changes to TWC, await an e-mail notice from TWC that the Security Report has been updated with the changes (which may take up to two business days), and review the updated Security Report in the CDER system.
3. Certify the Security Report (or updated Security Report, if applicable) in the CDER system.

NLF: Boards and grantees must ensure the following when establishing, reviewing, certifying, or changing CDER system user permissions:

- CDER system user permissions are necessary and appropriate for users' roles.
- Adequate separation of duties or compensating controls exist to safeguard grant funds with respect to CDER system user permissions.

LF: Boards and grantees may refer to the CDER system Security Verification training module for detailed instructions for performing the online security verification. The module is available on TWC's Cash Draw & Monthly Expenditure Report System web page at https://www.twc.texas.gov/agency/cash-draw-monthly-expenditure-report-system.

Ongoing CDER System Security Changes by Boards and Grantees

NLF: Boards and grantees must follow specific existing CDER system procedures, as shown below, to make changes during the year, as needed.

To designate or change a Security Administrator:

- Authorized personnel must e-mail the TWC Security Coordinator Designation Form to Cash Draw TA at cashdraw.ta@twc.texas.gov.
- The TWC Security Coordinator Designation Form is available on TWC's Cash Draw & Monthly Expenditure Report System web page at https://www.twc.texas.gov/agency/cash-draw-monthly-expenditure-report-system.

To establish CDER system access for a new user, use the following procedures.

- Go to the Cash Draw & Monthly Expenditure Reporting System page on TWC's website.
- Click "Request an Account."
- Type and submit the required information.

To add, change, or delete user permissions for CDER users, use the following procedures:

- Boards and grantees must follow the Board's or grantee's procedures for that entity's Security Administrator to establish user permissions.
- Permissions must be necessary and appropriate for users' roles.
- Permissions must provide for adequate separation of duties (or adequate compensating controls must exist) to safeguard grant funds, with respect to CDER system user permissions.

LF: In establishing user permissions, Boards and grantees may use the sample Cash Draw Operator Security Request form available on TWC's Cash Draw & Monthly Expenditure Report System web page at https://www.twc.texas.gov/agency/cash-draw-monthly-expenditure-report-system.

INQUIRIES:

Send inquiries regarding this WD Letter to fiscal.ta@twc.texas.gov.

REFERENCES:

None