



SBA Information Notice

TO: All SBA Employees & Lenders **CONTROL NO.:** 5000-1373
SUBJECT: Capital Access Financial System **EFFECTIVE:** February 4, 2016
(CAFS) Security

In compliance with SBA IT Security policy (SOP 90 47 3, dated 8/28/2012) and White House memorandum m-16-03, dated 10/30/2015 (<https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>), OCA has implemented automated security controls for the Capital Access Financial Systems (CAFS). The CAFS may be accessed at https://caweb.sba.gov/cls/dsp_login.cfm.

The security requirements that directly impact CAFS user accounts are listed below:

- Item 2a on page 21 of SOP 90 47 3 requires SBA to review information system accounts bi-annually to validate the accounts are still required. Account validations must confirm the following: (1) The user has a valid need-to-know/need-to-share, as determined by assigned official duties; and (2) The user still requires access for the intended system usage. The account certification process began the week of January 11th;
- Item 2d on page 21 of SOP 90 47 3 requires all accounts to be disabled after more than 60 days of inactivity;
- Item 2e on page 21 of SOP 90 47 3 requires all accounts to be terminated after more than 120 days of inactivity; and
- Item 1a on page 56 of SOP 90 47 3 requires all passwords to be changed every 90 days.

All account holders who are set up as an authorizing official (AO), Contracting Officer Representative (COR), and/or Supervisor received an email to log into the system between 1/11 and 2/25/2016 to certify accounts. To certify accounts use the instructions below:

1. Log into the system.
2. Select “Admin” on the navigation bar and navigate to Security -> Recertification Decision.
3. For each account holder managed by the AO/COR/Supervisor, review the roles under the account holder.
 - a. To deactivate an account, remove the check mark next to the name of the account holder.
 - b. To remove access, remove the check mark next to roles that are under the account holder.
 - c. If an account is valid and all roles are approved, do not select/deselect any items associated with the account holder.
4. After all accounts have been reviewed, select Submit. Once Submit is selected, all actions are final and immediate.

We recommend that all CAFS account holders log into their account monthly to review their profile. The instructions for accessing your profile are listed below.

1. Go to the production URL.
2. Log into the system.
3. At the top right, select the person icon.
4. Select “Update Profile.”
5. Update security questions, Job Classification, AO/COR/Supervisor, email address (NOTE CHANGING EMAIL ADDRESS REMOVES ALL SYSTEM ROLES FROM YOUR

EXPIRES: 2/1/17

PAGE 1 of 2

ACCOUNT), and/or Location ID (NOTE CHANGING LOCATION ID REMOVES ALL SYSTEM ROLES FROM YOUR ACCOUNT).

6. Press "Submit."

7. After the AO/COR/Supervisor approves the request, you will receive an email from cls@sba.gov that your account request has been approved. (Note: changing the AO/COR/Supervisor will result in your account being suspended until the AO/COR/Supervisor logs into the system to approve the request.)

What will be affected? Systems managed by OCA.

Who will be affected? Users accessing the following systems: CLCS (Centralized Chron System), SBA One, Electronic Lending System (ELIPS), Electronic Transaction (ETRAN) Origination, ETRAN Servicing, ETRAN Post Servicing (PSA), GPTS, ILPERs (Intermediary Lender Program Electronic Reporting System), LANA (Loan Name and Address), LAORS (Loan Accounting Report Systems), LINC Lender Opt In, MPERS (Microloan Program Electronic Reporting Systems), Micro Lender Application System, Partner Information System (PIMS), Surety Bond Guaranty, and Wizards/Loan Authorization.

If you need additional information, please send an e-mail to CLS@sba.gov for assistance.

Steve Kucharski
Director,
Office of Performance and Systems Management,
Office of Capital Access