LEADS Daily Briefing for April 10, 2020

LEADS 2000 Passwords

A LEADS 2000 password will expire after 35 days and must be changed at the first sign-in attempt after the 35 day. An expiration notice will appear on the log-on page when a user's LEADS 2000 password has expired. (Since the expiration notice appears under the name and password fields on the LEADS 2000 log-on page, it may not be visible when the user has the page set at half size. Therefore users should ensure the page is maximized when logging on so as not to miss the expiration notice.) When this occurs, the user must change his/her password.

No intervention from the LEADS Agency Coordinator (LAC) or LEADS 2000 delegate is necessary to change a user's password when it has expired. However, if the user attempts to sign-in to LEADS 2000 three times using the expired password, his/her access will be revoked after the third attempt. If this occurs, it is the responsibility of the agency's LAC or LEADS 2000 delegate to reset the user's password. For information on how to reset a password, please refer to the LEADS 2000 User Registry Manual (LEADS 2000 > LEADS Information).

LEADS 2000 passwords are not case sensitive and must contain exactly 8 characters, at least one of which must be a number but the number may not be the first character. Also, when changing a password users should be reminded that programming will not allow a password to be reused for 32 generations (approximately 2 years and 8 months based on a password being changed every 35 days). If a user attempts to reuse a recently used password, a LOGON FAILED - PASSWORD IS EXPIRED notice will be received. When this is the case, the user should simply change to a different password.

For assistance please contact the Help Desk at 866/LEADS-00.	
--	--

Operator's Initials	Date								