g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Any user accessing any Corps hardware, software or firmware, must have their Common Access Card (CAC) and a userid validated and maintained through the USACE UPASS system. Any CWBI user must also be granted permission and then authenticated through the Oracle database. Passwords for both network access and database access must be changed every 60 days. The CWBI system administrator must also change the Oracle CWBI passwords every 60 days. Each user is provided a role that assigns the minimum access that the user needs. Users of CWBI are government employees and contractors. Users are not required to possess a security clearance for system access and Foreign Nationals employed by USACE may access CWBI. All persons accessing CWBI participate in a periodic security training and awareness program. All personnel with management responsibility are aware of operational and security-related procedures and risks. All personnel designated as ADP I, II or III are subjected to a pre employment background investigation. User access is terminated when a user no longer requires access. Users are required to lock their computers when leaving their workstations unattended. Passwords are inhibited, overprinted or otherwise protected from unauthorized observation on terminals and video displays. Passwords for systems processing must be at least a fifteen character string using the 36 alphabetic-numeric characters and do not need to be randomly generated. At least two of the characters must be upper case alpha, lower case alpha, numeric and special characters. User logon-restricted access is monitored for unsuccessful user logon after three attempts, privileged user logon/access, and directory/file access. After three unsuccessful user logons, the userid is blocked from subsequent attempts. Regular applied patches to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's) prevent any new opportunities to compromise CWBI data. Partners are provided information through regularly scheduled file transfers accomplished via ftp or email across the RSN or Non-classified but Sensitive Internet Protocol Router Network (NIPRNET). Files transferred across the Internet/ NIPRNET are encrypted using a Virtual Private Network (VPN) or Advanced Encryption Standard (AES) 256-bit encryption.

Physical security consists of an access restricted area where the maintained server platforms are environmentally controlled and uninterruptible power supply protected. CWBI data is Unclassified-Sensitive Two (US2).

Security measures are tested annually.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A