CROMERR Success Story
Texas CEQ STEERS

The Texas Commission on Environmental Quality (TCEQ) received approval from EPA, under the Cross-Media Electronic Reporting Regulation (CROMERR), for modifications/revisions to their authorized programs that use or will use the State of Texas Environmental Electronic Reporting System (STEERS) to receive electronic reports. TCEQ submitted a consolidated CROMERR application to cover over 140 electronic reports under multiple EPA-authorized programs for drinking water, wastewater, air, and solid waste. These electronic reports include those requiring electronic signatures and "priority reports."

TCEQ designed STEERS as a flexible, modular system that allows TCEQ to add data reports with minimal effort. This provides TCEQ the ability to respond easily to future reporting needs. TCEQ plans to use the same security and compliance measures for all future reports. For example, the application includes a report that TCEQ is currently developing for air emissions inventories. Since this future report was included in their approved CROMERR application, TCEQ will not need to revise their application when it is ready to come online, unless they make changes that might impact CROMERR compliance.

Solution to Meeting CROMERR Requirements

The Texas STEERS system achieves CROMERR compliance by implementing the same business practices and system functions for all the programs supported by the system. For example, TCEQ requires all registrants to complete an electronic signature agreement (ESA) before using STEERS to submit electronic reports under any program. Identity-proofing of the registrants is provided in one of two ways: either they submit their ESA on paper with a wet-ink signature, or they use the Texas Online Authentication service which validates four pieces of personal information from at least two sources (one of those being the registrant-provided driver's license) to verify the user's identity information. In addition, the registration process requires the user to select and answer five challenge questions.

Each STEERS account is associated with specific program areas and with specific sites or facilities within those programs. Users must indicate for each program area and site combination whether they

For More Information on CROMERR Contact:
cromerr@epa.gov

http://www.epa.gov/cromerr/

have direct signature authority, or, if signature authority was delegated to them, who delegated it.

In order to access the system, users must execute a valid logon, which requires them to provide an account identifier, the associated password, and the correct answer to a challenge question. The combination of password and challenge question-answer provides two-factor authentication of the user's identity. These authentication measures also help ensure that no one other than the legitimate account-holder can change his/her registered password or e-mail address, since users wishing to change these items in their account profile must first successfully answer a challenge question.

Users execute electronic signatures on their reports by entering their passwords at the time of signature. While the signature process does not include a challenge question, the STEERS session time-out limit of 20 minutes helps ensure that the signer is the individual who entered the answer to a challenge question at logon. Upon receipt of the signed report, STEERS creates a hash of the copy of record (COR) using the SHA-256 algorithm; this hash serves to which binds identifying account information – including a hashed version of the password entered as signature – to the submission content. After each submission, STEERS sends an acknowledgment email to the address on file for the user submitting the document. STEERS also sends confirmation emails to other account holders with authorization for the same program at the same facility. STEERS confirms signature binding and document integrity for stored CORs by recalculating the hash and comparing it to the one generated at the time of submission.

STEERS maintains all CORs in a database system that has a robust, redundant backup mechanism. The database is backed up weekly, with an incremental backup performed daily. These backups are stored in a secure facility offsite.