



False Data Entry in DEERS

The entry of false information into the DEERS database is a serious security violation. All data input into the DEERS database **MUST** be based on and verified by official documentation. All transactions made in the DEERS database are audited and systematically traced back to the SSM or VO responsible for each transaction. Workarounds must NEVER be used to create or change a DEERS record in violation of Department of Defense policy.

For security purposes, an individual's password or PIN must NEVER be shared with anyone, including other VOs, SVOs, or SSMs. A VO must not log on to a RAPIDS workstation and allow another individual to make updates. A VO must never leave his/her VO CAC unattended in the VO smart card reader/encoder.

Any individual ignoring these warnings will have their SSM/VO capability IMMEDIATELY terminated and such conduct will be reported both to the appropriate DEERS/RAPIDS Service Project Officer and to a responsible individual or individuals in their local chain of command. Security compromises, especially in the area of positive identification, can result in serious consequences for the Services and the Nation.