Scientists Retreat Pre-meeting Security Area

- ***Our Goal:*** to help position our lab as an open, easily accessible international lab. Lower unnecessary barriers against accessing our resources internally or externally.
    - *User-friendly access control management technologies and removing our dependency on X.509 certificates.* What other technologies can provide privilege management and accountability at the same security & assurance level as certificates do? What are the access control requirements from our computing centers, VOs, Clouds and HPC centers? Traceability, isolation, privilege management, and so on? Can we satisfy these needs via different technologies?
    - *Close integration of trust federations into our infrastructure.* Enable external users to use their home credentials to authenticate themselves to Fermilab. Building trust between resource and identity providers is still evolving. Are federation-based technologies alone enough to replace certificates? ·
    - *More diverse resource providers connected through cloud gateways*. For example, HEPCLoud aims to connect Amazon, Google Clouds and HPC centers with our traditional grid computing resources. How to evaluate and maintain operational security in such connected environments? How should we evaluate the security of these environments? What is the trust relationship between our community and external providers? Where our responsibility in operational security ends and theirs starts.
    - *Commercial clouds and HPC centers each has fundamentally different access control models & technologies than our traditional grid environment.* We need a new access control model that is compatible with these technologies and translate our grid-based identity attributes into attributes consumable by the clouds and HPC centers. This need ties in well with the access control problem described above.