Identity Policy:

**Resolution:**

* Credentialing Service Provider collects minimum necessary information to begin the identity proofing process. CSP collects Full name (birth name), Date of birth, place of birth, address, as well as any other identifiable information like a DOD Identification number for military members.

**Validation:**

* CSP verifies the persons information by collecting two forms of government issued identification like driver’s license, passport, military ID, or birth certificate.

**Verification:**

* CSP utilizes facilities photography capabilities or face to face verification to match with the provided government issued identification in order to verify the individual’s identity.

**Password:**

* All systems-level passwords (e.g., root, enable, network administrator, application

administration accounts, etc.) must be changed at least every 90 days.

* All production system-level passwords must be part of the Information Security

administrated global password management database.

* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at

least every 90 days and cannot be reused the past 10 passwords.

* Passwords must not be inserted into email messages or other forms of electronic

communication.

* All user-level, system-level, and LEIN/NCIC access level passwords must conform to the

guidelines described below.

* Be a minimum length of eight (8) characters on all systems.
* Not be a dictionary word or proper name.
* Not be the same as the User ID.
* Expire within a maximum of 90 calendar days.
* Not be identical to the previous ten (10) passwords.
* Not be transmitted in the clear or plaintext outside the secure location.
* Not be displayed when entered.
* Ensure passwords are only reset for authorized user.

**Authentication device reset:**

* Requiring the claimant to complete a CAPTCHA before attempting authentication.
* Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed

attempts.

* Accepting only authentication requests that come from IP addresses from

which the subscriber has been successfully authenticated before.

* Leveraging other risk-based or adaptive authentication techniques to identify user

behavior that falls within, or out of typical norms. These might, for example, include use

of IP address, geolocation, timing of request patterns, or browser metadata.