Office of Communications (OC) – Standard Operating Procedures (SOP)

External Certificate Authority (ECA)

Purpose. All Military Community and Family Policy (MC&FP) employees, both government and contract personnel, are required to hold Department of Defense (DoD) certificates in order to operate within the Office of the Secretary of Defense (OSD) environment and MC&FP enclave. MC&FP would prefer new employees to obtain a Common Access Card (CAC). However, if this is not feasible, this SOP outlines the procedures for obtaining External Certificate Authority (ECA) certificate.

Scope and Responsibilities. This SOP details the responsibilities and procedures for all new MC&FP government staff and contract personnel in obtaining and renewing their ECA certificates. This also details storage and destruction of enrollment paperwork.

Procedures.

New ECA Certificate

- Send a request to the appropriate government manager with the following information:
  - Name
  - Email Address
  - Work Phone #
  - Operating system of the PC that will house the ECA certificates

- Government Manager will notify Brian Green (brian.green.ctr@mhf.dod.mil) of the information above with a signed e-mail, stating the user is approved for an ECA.

- The user must then contact Brian Green to begin the enrollment process which includes:
  - Web-conference with Brian, allowing him to perform the ECA enrollment and complete some configuration on the user's PC.
  - Establishment of a challenge password that the user MUST remember.
  - (Suggest that users maintain ECA information (challenge password and expiration date) in a secured file.)
  - **NOTE:** Users should notify Brian Green anytime they receive an email from VeriSign prior to execution of email instructions.

- The user's completed enrollment must be notarized and faxed to Brian Green at 208.567.8802. With his approval, the completed enrollment (all ORIGINAL documents) must then be mailed to:
  - Beth Riffle
  - MC&FP Office of Communications
  - 4000 Defense Pentagon, Rm 2E335
  - Washington, DC 20301
  - **NOTE:** If possible, hand delivery is preferable as it expedites the processing time.

- Upon Beth Riffle's receipt of the user's original documents, Brian Green will notify VeriSign.
- User will immediately notify Brian Green when VeriSign sends the user an email receipt.
- Brian Green will web-conference with user to obtain the ECA from VeriSign, back up the file and register it with the user's PC.
- ECA cannot be utilized by anyone other than the user it was established for.

Renewing existing ECA certificates

- VeriSign will automatically notify the user 30 days prior to expiration, at the email address specified in original enrollment request.
- User will notify Brian Green of pending expiration within 30 days of expiration.
- User and Brian Green will web conference to allow him to perform the re-enrollment.
- User will immediately notify Brian Green when VeriSign sends the email receipt.
- Brian will web-conference with user to obtain the ECA from VeriSign, back up the file and re-register it with the user's PC.

Staff Turnover

- Government manager is responsible for notifying Brian Green with a signed e-mail when an employee leaves so their certificates can be revoked.

Storage and Destruction

- Original enrollment documents for all users are to be maintained in a secured space due to Personal Identifiable Information (PII).
- When user transfers or has transitioned to a CAC, Brian Green will notify Beth Riffle who will shred the enrollment document.

Approval and Review. This SOP was approved by the OC Deputy Director on January 26, 2010 and remains in effect until superseded. OC management staff shall review this SOP annually at the start of each fiscal year or as needed for updates.