Sensitive and Classified Mission Programs

CAP doesn't traditionally conduct or support classified missions of a secret or higher nature itself, but it does support sensitive missions regularly, and some mission results support classified missions and customer needs. Members need to be familiar with the classification definitions and their associated access and guidance requirements below.

Classification Definitions

These definitions are quoted from DoD Directive 5200-1. Refer to the DoD Directive if information on higher classifications if needed.

- Unclassified controlled information shall be applied to information that requires protection for types of information that require application of controls and protective measures for a variety of reasons. Type of information that fall within this category include "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, “Law Enforcement Sensitive”, "DEA Sensitive Information", "Sensitive Information" as defined in the Computer Security Act of 1987, and information contained in technical documents.
- Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information. i.e. – CAP radio frequencies
- Information Security. The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.
- Access. The ability and opportunity to obtain knowledge of classified information, unclassified sensitive information, LE Sensitive, DEA Sensitive, etc. The proper clearance and/or background investigation granted by DoD, Law Enforcement Agency, CAP, etc will be needed for access. Agencies may require CAP members to sign a binding non-disclosure agreement before granting members access.
- Need to know – CAP members who have been authorized by a customer/tasking agency, posses the proper access level, and designated CAP authority will be granted access to unclassified or classified mission information. The customer may restrict CAP personnel who have a need to know. Member’s involvement in a particular mission will determine need to know. i.e. – IC working a sensitive mission. Mission information will not be shared with personnel that do not have a “need to know”.
- Close Hold/Sensitive – Mission information that is unclassified but must be safeguarded. Loss of Close Hold or Sensitive information would compromise ongoing operations for a supported agency. Members will safeguard Close Hold/Sensitive unclassified information to prevent deliberate or accidental disclosure.
- Classified missions will receive their designation from the request/tasking agency and not designated or derived by CAP. CAP may designate an unclassified mission as Sensitive but Unclassified or Close Hold. Requesting agencies may designate a mission Law Enforcement Sensitive, DEA Sensitive, or Sensitive Information.

Classification Access and Guidance

DoD Directive 5200-1 outlines the requirements and guidance for access and handling of classified materials and information. The following outlines the basic guidance for CAP missions:

- CAP mission information will be handled in accordance with the level of classification assigned to the mission.
- Only CAP members with a proper clearance in the CAP/CAP-USAF database and a need to know will have access to classified information. Members with a need to know for mission support shall have access to Unclassified Sensitive information as defined in CAPR 60-3. Need-to-know is a determination made by an

authorized holder of classified or sensitive information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function. A member's rank and/or grade does not automatically entitle access to Unclassified/Sensitive, Unclassified/Close hold, or classified mission information. A need to know and proper clearance determines a member's access to information.

- CAP members will mostly work with Unclassified "For Official Use Only", "Sensitive But Unclassified", "DEA/Law Enforcement Sensitive" information. Only CAP members that hold an appropriate DoD Security Clearance along with a need to know will be involved in classified missions on a case by case basis.
- CAP members will mark documents and email traffic to insure that sensitive mission traffic is handled appropriately. Unclassified documents containing DEA/Law Enforcement Sensitive information shall be marked "DEA or Law Enforcement Sensitive" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one). Unclassified documents containing FOR OFFICIAL USE ONLY shall be marked in a similar manner. Each part of electrically transmitted messages containing FOUO or LE Sensitive information shall be marked appropriately. Unclassified messages containing FOUO / LE Sensitive information shall contain the abbreviation "FOUO or LE Sensitive" before the beginning of the text. Files attachments will be similar marked.

CAP Personnel with Clearances Already

Some CAP personnel have security clearances already because of their full-time jobs, either from DoD or another federal agency. CAP has very few missions requiring personnel with security clearances at this time, and is not normally involved in investigations or other requirements to get or maintain security clearances. That said, occasionally there are missions that customers would prefer to use members with security clearances, and we have tools in place within e-services for members to input information on their existing security clearances so that CAP-USAF can then validate them for potential usage, allowing CAP to have a pool of personnel with valid security clearances when necessary. Personnel with current and valid security clearances can input this information by logging into e-services, clicking on Review/Edit My Info under the My Info section in the top center of the page, clicking on Security Clearance in the left menu, and then submitting the Agency, Type, and Date the investigation was closed. Information will show as Pending until verified by the issuing agency. Personnel submitting a clearance from a non-DoD agency must email the Federal Agency point of contact to the Security Clearance Group at secclear@capnhq.gov so that CAP-USAF can contact the POC to validate the clearance appropriately.

For more information on Sensitive and Classified Mission Programs:
Contact NHQ CAP/DO at 888-211-1812, extension 303 or email do@capnhq.gov.