Chapter 17

Emergency Action Plan (EAP)

1. Natural Disasters. Natural disasters includes fires, floods, hurricanes, and any phenomena that would result in the inadvertent loss, compromise, or destruction of classified material. When such a situation occurs, the senior Marine present will execute the Emergency Action Plan (EAP).

a. Fire after duty hours. Should a fire occur around or within the building where classified or COMSEC is stored, the custodian of the classified or COMSEC will:

(1) Notify the Fire Department and Military Police by dialing "911" and report the location and extent of the fire.

(2) If the fire occurs during duty hours, secure all classified and COMSEC material in the safe and secure the vault door.

(3) If the fire occurs after duty hours, ensure the Vault or Secure Room door which stores classified or COMSEC is secured before leaving the area.

(4) If safe, use all local means to extinguish or control the fire until the fire department arrives. Fire extinguishers are located throughout the building.

(5) If after duty hours, and as soon as possible, notify the Security Manager.

(6) Under no circumstances will anyone subject themselves or their subordinates to possible death or injury to protect classified or COMSEC material from fire.

(7) When the Fire Department/Military Police arrive, they will immediately be informed of and admitted to the secure areas. Efforts will be made to get names and identification numbers of all emergency personnel going into secure areas or being exposed to classified or COMSEC material only after the emergency is over.

(8) The Security Manager/Assistant or Classified Custodian will, to the maximum extent possible, ensure that only emergency personnel are allowed into secure areas. When given the "ALL CLEAR" signal from emergency personnel, the vault will be locked and two guards will be placed in the secure area until the Security/Assistant Manager performs a post-emergency inventory.

(9) If the intensity of the fire is such that the area must be abandoned, maintain a surveillance of the general area to prevent unauthorized persons from entering, to the best of your ability.

b. Hurricanes, Floods, and other Natural Phenomena. The danger presented by these conditions are not likely to be as sudden as that presented by fire. The primary objective in case of hurricane, flood, etc., is to secure and waterproof classified material and computers to protect them from wind, water, or destruction until the emergency has passed.

(1) Prior to hurricanes the Security Manager, Security Assistant, or Classified Custodian will waterproof all classified or COMSEC material and gear in safes. All classified computers will be unplugged and waterproofed with plastic as necessary. All other logs, documents, and other important papers will also be secured in waterproof containers.

(2) If there is damage to the CMCC Vault from a hurricane, flood, or other phenomena, the Station Duty Officer (SDO), or other person on the scene, will immediately contact the Security Manager or Security Assistant to inform them of the extent of damage.

(3) Two persons will be posted, if necessary, as a guard force to prevent unauthorized access to classified material until CMCC personnel arrive.

(4) The CMCC will coordinate the removal of classified material, if required, to a location designated utilizing the Emergency Evacuation Cards located on the inside left wall of the CMCC Vault.

2. Hostile Actions (see Emergency Destruction Plan). Hostile actions include, bomb threats, riots, or civil uprisings. In all cases, the assumption will be made that classified or COMSEC material is a target. All actions must be directed to prevent unauthorized personnel from gaining access to classified or COMSEC material by securing or evacuating the material as conditions dictate. There are three threat stages of hostile action emergencies. These stages will be carried out by CMCC personnel only.

a. Stage One – Force Protection Condition – Bravo.

(1) Threat source - Operations in high risk environment.

(2) Time frame - Several days to several months.

(3) Action - Precautionary Emergency Protection as outlined under Terrorist Actions below.

b. Stage Two - Force Protection Condition – Charlie.

(1) Threat source - Probability of hostile attack.

(2) Time frame - From one to several days.

(3) Action - Possible Emergency Evacuation as outlined under Emergency Evacuations below.

c. Stage Three - Force Protection Condition – Delta.

(1) Threat source - Attack by hostile forces.

(2) Time frame - Imminent.

(3) Action - Immediate Emergency Protection or Evacuation as outlined under Terrorist Actions and Emergency Evacuations below.

d. Bomb Threat. In the event of a bomb threat, the Provost Marshal's Office (PMO) will be notified by dialing "9-1-1". Classified and COMSEC material will be secured in the CMCC safe. The safe will be locked and all

classified/COMSEC material accounting records will be removed from the building. Personnel will wait outside the building at a safe distance until the arrival of the military police and Explosive Ordnance Disposal (EOD) Team. The building will not be re-entered until the "ALL CLEAR" signal is given by EOD personnel.

3. Terrorist Actions (see Emergency Action Plan). Acts of terrorism range from threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings, cyber-attacks (computer-based), to the use of chemical, biological, and nuclear weapons. All actions must be directed to prevent unauthorized personnel from gaining access to classified material by securing, or evacuating the material as conditions dictate. There are five threat stages of terrorist action.

a. Force Protection Condition – Normal. FPCON NORMAL applies at all times as a general threat of terrorist attacks, hostile acts, or other security threats always exists in the world.

(1) Educate command personnel on the terrorist and hostile adversary threats, deterring and detecting these threats, and reporting indications of these and other suspicious activities, to maintain a level of protection the Secretary of Defense requires for all DoD elements and personnel against terrorist attacks and hostile acts.

(2) Ensure personnel are knowledgeable on terrorist and hostile actor threats; understand the individual actions they can take to protect themselves and others from terrorist attack; know procedures for reporting suspicious activities and incidents; deter and detect general, non-specific threats of terrorist attacks and hostile acts; and prepare to implement additional FPCON measures designed to delay, deny, and defend against these threats.

(3) Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

b. Force Protection Condition – Alpha. FPCON ALPHA applies to a non-specific threat of a terrorist attack or hostile act directed against DoD elements and personnel.

(1) Checking communications with designated emergency response or command locations.

(2) Reviewing and updating emergency response procedures.

(3) Providing the public with necessary information.

c. Force Protection Condition – Bravo. FPCON BRAVO applies when an increased or more predictable threat of a terrorist attack or hostile act exists and is directed against DoD elements and personnel. In addition to the previously outlined protective measures, the following may be applied:

(1) Increasing surveillance of critical locations.

(2) Coordinating emergency plans with nearby jurisdictions.

(3) Assessing further refinement of protective measures within the context of current threat information.

(4) Implementing, as appropriate, contingency and emergency response plans.

d. Force Protection Condition – CHARLIE. FPCON CHARLIE applies when a terrorist or hostile act incident occurs within the commander's area of interest (AOI), or intelligence is received indicating a hostile act or some form of terrorist action or targeting against DoD elements, personnel, or facilities is likely. In addition to the previously outlined Protective Measures, the following may be applied:

(1) Coordinating necessary security efforts with armed forces or law enforcement agencies.

(2) Taking additional precaution at public events.

(3) Preparing to work at an alternate site or with a dispersed workforce.

(4) Restricting access to essential personnel only.

e. Force Protection Condition – DELTA. FPCON DELTA applies when a terrorist attack or hostile act has occurred or is anticipated against specific installations or operating areas. In addition to the previously outlined protective measures, the following may be applied:

(1) Assigning emergency response personnel and pre-positioning especially trained teams.

(2) Monitoring, redirecting or constraining transportation systems.

(3) Closing public and government facilities.

4. Emergency Evacuation. Emergency evacuation is that action taken to move classified material to a safe place to prevent unauthorized access caused by fire, hurricane, flood, other natural phenomena, hostile action, or terrorist action. Emergency evacuation will only be executed when directed by the Installation Commander or Security Manager. The Primary Classified Storage area will be the CMCC Vault located in Building 601. During non-working hours and when directed, the Command Duty Officer (CDO) will:

a. Attempt to contact CMCC personnel and the Security Manager using the Emergency Recall Roster (located in the CDO Binder).

b. The Security Manager or Assistant Security Manager must appoint at least two persons to evacuate the classified material, and contact military police to provide armed escort for the evacuation.

c. Ensure a government vehicle with driver is readily available for pick-up and delivery of classified material during evacuation.

d. Post a military policeman armed guard at the vault entrance and vehicle until all classified material is loaded onto the government vehicle.

e. After all classified material has been gathered and packed, the armed guards will escort and protect the total evacuation of all classified material to include unloading and safeguarding it at the new location.

5. Emergency Protection. Emergency protection actions include collecting all classified material not needed for immediate operational use, and securing them in the CMCC Vault and safe. Emergency protection procedures will only be executed when directed by the CO, Security Manager, or other competent authority.

a. All classified material will be locked up in the safe.

b. All other publications, logs, and correspondence will be packed and prepared for evacuation.

c. Any other protection actions deemed necessary by the Security Manager will also be completed during this time.

6. Emergency Destruction Plan for COMSEC. When a hostile action occurs, the decision to enact the complete emergency destruction plan will be made by the CO, Security Manager, or COMSEC Manager. Utilizing the Accountable Items Summary, (located in the Chronological file in the CMCC Office), to account for all material prior to destruction. Once all material has been accounted, destroy the following material in the order listed below:

a. CMCC Safe.

(1) Open the CMCC safe and locate the "gray box" inside the drawer one and destroy "all" the contents of the "gray box" using the "yellow" sledge hammer located inside the CMCC vault.

b. COMSEC Aids.

(1) All COMSEC Aids are in the drawer one of the CMCC safe. These items will be destroyed using the "yellow" sledge hammer located inside the CMCC vault.

c. Equipment.

(1) Make a reasonable effort to evacuate equipment, but the immediate goal is to render it unusable and unrepairable.

(2) "***Zerorize***" all keyed cryptographic equipment.

(3) Remove and destroy readily removable classified elements.

(4) Remove the KSV 21 card from all STE phones and evacuated. If evacuation is not possible, the KSV 21 will be destroyed using the "yellow" axe located in the CMCC Vault.

(5) The Management Client Node (MGC) computer and all data contained on the hard drives is classified. If the computer cannot be evacuated, then the hard drives are removed and destroyed using the "yellow" sledge hammer located in the CMCC Vault.

(6) If Advance Key Processor (AKP) is not capable of being evacuated, ***Zerorize*** AKP. **(Never during a drill!)**