



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

3500
G-3/5
AUG 23 2017

COMMANDING GENERAL'S POLICY LETTER 07-17

From: Commanding General
To: All Commanders, Marine Corps Installations East-Marine Corps Base, Camp Lejeune and General and Special Staff

Subj: COMMANDER'S CRITICAL INFORMATION REQUIREMENTS REPORTING

Ref: (a) MCO 3504.2A
(b) COMMCICOM Policy Letter 6-15 of 27 Jul 15

Encl: (1) MCIEAST-MCB CAMLEJ Commander's Critical Information Requirements List

1. Purpose. To establish Commander's Critical Information Reporting (CCIR) policy for Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ) commands.

2. Information. In accordance with the references, MCIEAST-MCB CAMLEJ and subordinate commands must inform higher headquarters when specified events occur. In some cases the Operations Event/Incident Report (OPREP-3) process will be initiated and a message will be required. This policy letter formally establishes the CCIR's for the Commanding General (CG), MCIEAST-MCB CAMLEJ.

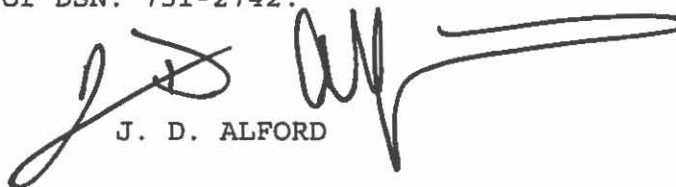
3. Action

a. All MCIEAST-MCB CAMLEJ installations and subordinate commands will ensure familiarity with this policy letter and the references.

b. All Command Duty Officers, Officers of the Day, and Squadron Duty Officers will review these CCIR's and be prepared to take appropriate actions if a CCIR event occurs.

c. All commands will ensure appropriate procedures are in place to report any CCIR event.

4. Point of contact is the MCIEAST-MCB CAMLEJ Director of Operations and Plans at (910) 451- 2742 or DSN: 751-2742.


J. D. ALFORD

Copy to:
COMMCICOM G-3/5/7

MCIEAST-MCB CAMLEJ Commander's Critical Information Requirements List

CCIR is information that must be brought to the CG's attention immediately. (Information that you would wake the CG to tell him.)

Commanders can report any CCIR directly to the CG. The Chief of Staff will also be notified who will verify the CCIR and direct further action. (Call the CG, if not already been notified, the Deputy Commander, recall staff members, and execute OPREP-3 reporting procedures.)

CCIRs are listed below as: Priority Intelligence Requirements, Friendly Force Information Requirements, and Essential Elements of Friendly Information. These CCIRs are common to MCIEAST-MCB CAMLEJ and Marine Corps Installations Command.

Per reference (b), there are time constraints associated with reporting to MCICOM. These constraints are noted in parenthesis following each CCIR. (Immediately/12 Hours/24 Hours)

PRIORITY INTELLIGENCE REQUIREMENTS (PIR)

PIR-1: HOSTILE ACT OR PHYSICAL THREAT (Immediately)

Examples: Report terrorist attack, surveillance, assassination, physical infiltration, and significant political/criminal subversion.

PIR-2: HOSTILE INFORMATION THREAT (Immediately)

Examples: Report suspicious/hostile computer network activity that isolates MCIEAST-MCB CAMLEJ installations or tenants, impedes mission performance, or affects/places at risk installation systems or classified data.

PIR-3: ENVIRONMENTAL THREAT (Immediately)

Examples: Report environmental conditions such as destructive weather or pandemics that will have a significant and degrading impact upon installations and tenant commands activities within the next 72 hours.

FRIENDLY FORCE INFORMATION REQUIREMENTS (FFIR)

FFIR-1: FATALITY/SERIOUS INJURY/HOSPITALIZATION OF PERSONNEL ASSIGNED TO MCIEAST INSTALLATIONS OR KEY INSTALLATION PERSONNEL (Immediately)

Examples: Report the injury or death of Commanding Officer or Executive Officer, principal staff, or Commander of a tenant organization (Mission Impact and/or Media Interest.)

FFIR-2: OPERATIONAL SUPPORT AIRCRAFT (OSA) RED STRIPE, OSA AVIATION MISHAP OR AN OPERATIONAL FORCES AVIATION MISHAP WHICH OCCURS ABOARD AN MCIEAST INSTALLATION (Immediately)

Examples: Any Class A, B, or C Mishap of an Operational Support Aircraft (OSA) or any Red Stripe message affecting OSA. An operational forces mishap which occurs at an air station or while conducting training at a MCIEAST installation, facility or range.

FFIR-3: MILITARY SUPPORT TO CIVIL AUTHORITIES (12 Hours)

Examples: Report requests for Defense Support to Civil Authorities (DSCA), any actions taken under Immediate Response Authority by an installation, or any mutual aid support where Marine Corps emergency service assets are not available for more than two hours for response aboard the installation.

FFIR-4: CHANGE IN SECURITY/READINESS/PROTECTIVE POSTURE (Immediately)

Examples: Report changes in Installation Force Protection Condition, Tropical Cyclone Condition, Information Control Condition, in the Local/Regional/National Homeland Security Alert Levels or receipt of a BLUE DART message.

FFIR-5: INSTALLATION READINESS DEGRADATION (24 Hours)

Example: Report any changes in readiness status or when the Commander's overall mission assessment or any command task is degraded in assessment to "NO" (Not Mission Capable) within Defense Readiness Reporting System (This will be a staff action during regular working hours.)

FFIR-6: HIGH INTEREST REPORTS/SIGNIFICANT MEDIA INTEREST (Immediately)

Examples: Report any OPREP-3 level events, mishaps, incidents, or allegations of criminal activity with significant impact on security, safety, sustainability, damage to property, or great potential for public/media interest.

FFIR-7: OFF BASE INFLUENCE (24 Hours)

Examples: Report any threat, activity, or event, (terrorist attack, natural disaster, or widespread power outage), from the immediate community or an adjacent military installation that will have a direct impact on any MCIEAST-MCB CAMLEJ installations mission, critical infrastructure, or manpower.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI)

EEFI-1: CRITICAL INFRASTRUCTURE (24 Hours)

Examples: Report degradations or risks to capabilities, (SPOD/ports, APOD/airports, railroads, road networks, or bridges), that provide critical deployment, sustainment or re-deployment support to the operating forces.

EEFI-2: COMMUNICATIONS SYSTEMS (24 Hours)

Examples: Report OPSEC violations, exploitation of or attacks against the design, configuration, and access policies and procedures for voice and digital communications systems.

EEFI-3: LOGISTICS INFORMATION (24 Hours)

Examples: Report exploitation of, any risks to, or attacks against the schedule, quantities, types of supplies, or customer information for logistics functions.

EEFI-4: FORCE DEPLOYMENT PLANNING AND EXECUTION (24 Hours)

Examples: Report exploitation of or attacks against the detailed training and deployment schedules for installation commands or tenant and visiting units that are training in preparation to deploy.