UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASE
814 RADFORD BLVD ST 20302
ALBANY GA 31704-0302

MCLBAO 3504.1
OTD/MA

JAN 30 2015

MARINE CORPS LOGISTICS BASE ALBANY ORDER 3504.1

From: Commanding Officer
To: Distribution List

Subj: COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (C4I) THREAT INFORMATION SHARING SUITE STANDARD OPERATING PROCEDURES

Ref: (a) SECDEF Memorandum, OSD 07688-10, "Final Recommendation of the Fort Hood Follow-on Review", 18 Aug 10
(b) MARFORNORTH FRAGO 001 to MFN OPORD 08-1, "Threat Information Reporting Requirements", DTG: 091958Z AUG 12
(c) MARADMIN 646/13 of 9 Dec 13
(d) MCIEAST-MCB CAMLEJO 3040.1A
(e) MCICOM Policy Letter 3-13 of 11 Jun 13
(f) MCO 3504.2A
(g) MFN AT OPORD 08-01
(h) USNORTHCOM INST 10-211, "Operational Reporting", 1 Dec 06
(i) MCIEAST-MCB CAMLEJO 3504.1

Encl: (1) MCLB Albany C4I Suite Mandatory Reporting Categories

1. Situation

a. Purpose. This Order provides direction and guidance for the use of the United States Marine Corps (USMC) Threat Information Sharing C4I Suite in monitoring and disseminating threat information in the Marine Corps Logistics Base (MCLB) Albany, Area of Operations (AO). The procedures outlined within this Order are not intended to replace local command reporting requirements, but to ensure that higher, adjacent, and supporting units are informed of appropriate threat information.

b. Background

(1) An independent review of the events surrounding the 2009 Fort Hood Shooting identified gaps in Department of Defense's ability to rapidly communicate unclassified and classified threat information across the enterprise.

(2) The USMC adopted the Navy's existing C4I Suite as the service wide solution to the Secretary of Defense-directed threat information sharing capability requirements set forth in reference (a).

(3) Reference (b) provided initial direction and guidance for use of C4I in the dissemination of threat information. Reference (c) directed the use of C4I as a USMC-wide threat information sharing tool.

(4) The use of the C4I Suite does not replace current Operational Report-3 (OPREP-3) requirements, per references (d) through (h). OPREP-3s, or information extracted from OPREP-3s, shall be posted in the C4I Suite as appropriate, ensuring all Personally Identifiable Information (PII) and information designated as Law Enforcement Sensitive (LES) is omitted.

2. Mission. To detect, deter, defeat, and mitigate threats and hazards in the MCLB Albany AO by providing near real-time threat and hazard related information concurrently across all levels of command, enabling commanders to take appropriate actions at the lowest possible level.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. MCLB Albany shall use the USMC C4I Suite to collaborate with other Marine Corps and Navy commands in sharing of timely threat and hazard information to facilitate situational awareness of emerging threats and hazards, which will enable more informed risk-based decisions. End State threats and hazards are deterred and/or mitigated before significant casualties or damage is suffered.

(2) Concept of Operations

(a) In accordance with reference (c), directed divisions shall monitor the C4I Suite, using audible and visual alarm functions, to immediately receive and/or report threat information.

(b) Per reference (c), 24/7 monitoring capabilities such as Police Departments, Operations Centers, or on-site duty officers, shall ensure 24/7 monitoring of C4I Suite to immediately receive and/or report threat information.

(c) Per reference (c), the following divisions, branches, and sections shall establish C4I Suite user accounts: Mission Assurance personnel; Law Enforcement personnel; Security and Emergency Services personnel; Emergency Operations Center personnel; Crisis Action Team members; Intelligence personnel working in support of Mission Assurance and Law Enforcement; Emergency Managers; and other military, civilian, or contractor personnel deemed essential in support of mission requirements.

(d) This Order shall be used in conjunction with the references and other current regulations and directives to ensure compliance with established policies and procedures and higher headquarters (HHQ) guidance. Deviations from procedures and instructions must be approved by, or referred to, the Commanding Officer, MCLB Albany.

b. Tasks

(1) Director, Operations and Training Division (OTD)

(a) Serve as the office of primary responsibility for the C4I Suite.

(b) Ensure the appropriate Mission Assurance personnel establish C4I Suite user accounts, per reference (c).

(c) Ensure the C4I Suite is monitored during normal working hours to immediately receive threat information and enter reports into the C4I Suite, as required.

(d) Designate the appropriate key MCLB Albany staff, Higher Headquarters (HHQ) and local, state and federal authorities are immediately notified of urgent threat information that has a direct impact on the MCLB Albany AO.

(e) When the installation Emergency Operations Center (EOC) is activated for crisis situations, ensure EOC personnel provide 24/7 monitoring of C4I Suite for receiving and/or reporting threat information per the enclosure.

(f) Assist and maintain the establishment of C4I Suite user accounts for MCLB Albany C4I Suite users, as required. Be prepared to provide the HHQ as required.

(2) Director, Public Safety Division (PSD)

(a) Designate the appropriate Marine Corps Police Department and Fire Emergency Services personnel establish C4I Suite user accounts, per reference (c).

(b) Ensure Emergency Service Dispatchers and Desk Sergeants maintain 24/7 monitoring of the C4I Suite to immediately receive threat information and earlier threat reports into the C4I Suite, as required per the enclosure. Ensure the appropriate key MCLB Albany staff is immediately notified of urgent threat information that has a direct impact on MCLB Albany AO.

(c) Coordinate with Mission Assurance for support in establishing accounts.

c. Coordinating Instructions

(1) C4I Suite Account Establishment. Designated users of the C4I Suite shall establish unclassified user accounts on the Non-secure Internet Protocol Router Network (NIPRNET). Personnel with access to the Secret Internet Protocol Router Network (SIPRNET) shall establish classified accounts on the SIPRNET.

(2) Training and Exercise. The following C4I Suite website shall be used for training and exercises: https://c4isuitetraining.atfp.cnic.navy.mil/usmc/pages/index.aspx

(3) Data Entry Restrictions. Communications on the C4I Suite shall have appropriate classification markings. PII and LES information shall not be posted on the C4I Suite at any time. Information posted on the NIPRNET C4I Suite shall be maintained at the Unclassified/For Official Use Only level. A NIPRNET C4I Suite notice alert can be used to refer users to classified sources such as the SIPRNET C4I Suite or SIPRNET message traffic.

(4) C4I Suite Functions and Use

(a) Urgent Notices

1. The Urgent Notices function shall be used to share significant threats/incidents (usually requiring immediate action/reports) such as OPREP-3 Blue Darts, terrorist attacks, or all-hazards events that have potential to significantly impact missions. Reference (b) sets forth well as the staff sections responsible for reporting categories, as well as the staff sections responsible for reporting them, are listed in enclosure (1) to this SOP.

2. The urgent notices function has four subcategories: Antiterrorism Force Protection (AFTP), Multiple Threat Alert Center (MTAC), Operations (OPS), and Administrative (ADMIN). The Marine Corps shall use only the ATFP notice category for reporting.

(b) Routine Notices

1. The routine notices function shall be used for other reportable events and incidents of non-urgent/non-actionable nature.

2. The routine notices function has four subcategories: OPREP-3 Incidents, Other Reportable Incidents, Ops, and ADMIN. The Marine Corps shall only use the "Other Reportable Incidents" notice category.

(c) Audio Visual Alerts. The C4I suite includes audio and visual alert capabilities to alert users of new notices posted in the database. To set these alerts, click on "Change Setting" under both urgent and routine notices and, at a minimum, check the boxes next to "All USN" Users shall set the recipient filters each time they log into the C4I suite.

(d) Recipient Filters. The C4I Suite recipient filters allows users to choose the commands from which they want to receive notices. To set the recipient filters, click on "Change Settings" under both urgent and routine notices and, at a minimum, check the boxes next to "All USMC" and "All USN" Users shall set the recipient filters each time they log into the C4I Suite.

(e) Creating Urgent or Routine Notices. To create a notice, click on "Add New Item" under the urgent or routine notices functions, and complete the following required information:

1. Short Title. Enter a short title that contains the event and classification level. Example: MCIEAST-MCB Camp Lejeune Bomb Threat (U//FOUO).

2. Status. Select "Open" from the drop-down menu for all initial reports. Select "Closed" when the notice is no longer relevant or within 72-hours of incident exposure.

3. Notice Type. Select the appropriate notice type from the drop-down menu. The Marine Corps shall use only the "AFTP" category for urgent notices, and the "Other Reportable Incidents" category for routine notices.

4. Mission Area. Select the appropriate mission area from the drop down menu. The mission areas correspond to the Defense Readiness Reporting System-Marine Corps (DRRS-MC) reporting categories to facilitate linkage between the two systems at a later date. The selection of a DRRS-MC related mission area will not be applicable for all reports, but should be included when possible. Including this information does not fulfill the DRRS-MC reporting requirements.

5. Recipients. Carefully select recipients for the notice. Ensure only Regions/Commands which need the information or would benefit from it are selected. The selection of the "All" categories shall only be used when the report is of global, enterprise-wide interest.

6. Significant Details. Enter a brief narrative of the event, at a minimum, the narrative shall contain the basic, essential information (who, what, when, where, and why) to allow users to quickly assess the incident. Formal command reports such as OPREP-3s can be copied and pasted into this section, or the report can be attached with the statement "See attached document" in the data field. If urgent, event notification shall not be delayed due to the lack of certain details of the event.

7. Actions Taken. Enter a brief description of actions taken by the reporting command.

8. Message Date Time Group (DTG). Enter the DTG of any relevant naval messages submitted for the incident. The date and time shall be in ZULU format.

9. Incident Type. Enter the reason for the report (Example: Bomb Threat, Suspicious Person, Unauthorized Access, etc).

10. Incident Time. Enter the date and time of the incident. The date and time shall be ZULU format.

11. Incident Location Title. Enter the general location of the incident.

12. Location. Enter the specific location of the incident. The location can be a street address, a latitude/longitude coordinate, a postal zip code, or a well-known geographic feature (example: White House). If a detailed location is entered in this data field, the location will be automatically plotted on the map. Alternatively, the location can be directly entered by clicking on the map.

13. Source of Information. Enter the name of the organization that provided the incident information.

14. Source Credibility. Select the source credibility rating from the drop-down menu.

15. POC Name. Enter the name of the individual submitting the report.

16. POC Command. Enter the organization of the individual submitting the report.

17. POC Phone. Enter the phone number of the individual submitting the report.

18. POC Email. Enter the email address of the individual submitting the report.

19. Adding Attachments. Click on "Attach File" at the top of the page. Click on "Browse" to locate the document in your computer files. Double-click on the document to add it to the notice.

20. Save. Click on "Save" after all required information has been inserted.

21. Updating/Editing Notices. To provide to a notice, open the original notice and insert "UPDATE 1" in the "Significant Details" or "Actions Taken" data fields, followed by a brief narrative of the update. Do not create a new notice for the updated information. Updates should be made as soon as possible. There is no limit to the number of times a notice can be updated. Indicate additional updates by numbering them (Example: UPDATE 1, UPDATE 2, UPDATE 3, etc.). When a notice is updated or edited, it triggers a visual and audio alert for users monitoring the C41 Suite. The person entering the information must click on "Update Now" at the bottom of the notice function to see the visual and audio alerts.

22. Closing Notices. Notices should be closed as soon as they are no longer relevant, or within 72 hours of incident closure. Closed notices are archived, but remain accessible in the C4I Suite.

(f) Chat

1. Chat is used as an instant coordination and collaborative tool to provide HHQ and adjacent commands situational awareness of events. Chat may be used for initial reporting of time-sensitive information, but shall be followed by an urgent or routine notice entry, as required.

2. Chat shall not be used as a formal means to report incidents, or transmit orders and reports (e.g., change in Force Protection Conditions or Situation Reports), in lieu of using urgent or routine notices.

3. Chat input shall be short, professional, and mission-oriented, using only standard terminology.

4. During initial C4I Suite login, users shall open Chat by clicking on the "Start Button". Opening Chat will allow activation of an audible alert tone to alert the user when a Chat is received.

(g) Operational Status Panel

1. The Operational Status Panel displays the category columns with color-coded icons to provide commanders a quick reference of category dispositions. Changes in operational status shall be made as soon as possible. Amplifying information for clarification shall be addressed in the panel field's comment box by opening the panel and clicking on "Edit Item" The following defines the categories for each panel column:

a. Updated. This column indicates the currency of the information in the remaining columns

b. Force Protection Condition (FPCON) Directed. This column displays the FPCON directed by HHQs.

c. FPCON Current. This Column displays the current FPCON level at each command.

d. Additional Random Antiterrorism Measures Implemented (ADDL RAMS IMP). This column displays HHQs-directed RAMS in response to a threat. This is not associated with installations' RAM programs.

e. OPS. This column displays the status of Command Operations Centers' ability to support the Force Protection (FP) mission.

f. Task Critical Assets (TCA). This column displays the ability of identified TCAs to support mission requirements. The purpose of this panel is to alert HHQ and adjacent commands of an incident involving an identified TCA. No information on the specific TCA shall be posted on the NIPENET C4I Suite. TCA comments on the NIPRNET C4I Suite should read "See SIPRNET C4I Suite for details" or "See Marine Corps Critical Asset Management System Next Generation for details".

g. Installation Emergency Management (IEM). This column displays the ability of installations to meet the required tasks outlines in Marine Corps Order 3440.9.

h. Environmental (Environ): This column displays the impact that man-made or natural hazards have on the commands ability to support the FP mission.

i. In-Transit Security-Official (ITS-OFF). This column displays the status of USMC or USMC-chartered ships, aircraft, and USMC elements that could present lucrative terrorist targets, typically those elements traveling on orders and consisting of more than 50 personnel conducting both intra-theater and inter-theater transit within the United States Northern Command (USNORTHCOM) AOR. Change of status panel indicates a loss of accountability or an event that is reportable under service and Combatant Commander (COCOM) requirements.

j. In-Transit Security-Non-Official (ITS-NON-OFF). This column displays the status of USMC personnel individuals or small groups of less than 50 traveling in an official or non-official status outside the continental United States in the USNORTHCOM AOR. Change of status panel indicates the loss of accountability or an event that is reportable under service or COCOM requirements.

(1) Definitions of Color Coded Status Boxes:

(a) Green = System is functioning without noted degradation.

(b) Yellow = Significant or noted degradation to capabilities with mitigations in place.

(c) Red = Major unmitigated degradation adversely impacting installation operations and/or readiness.

(h) One Clear Picture (OCP). OCP data can be accessed by clicking on the OCP tab at the top of the C4I Suite main page. OCP enables users to visualize important operational information in a geographically referenced display to facilitate collaboration, assist in decision making, increase situational awareness, and enable incident trend analysis. Users may view specific OCP data by selecting the various map layers. Additional map layers may be determined for Enterprise situational awareness and added accordingly, either permanently or temporarily, such as for an exercise or training event. OCP also offers a plume-modeling capability.

(i) Document Libraries and Links. Document libraries and useful links are available on the lower left portion of the C4I Suite. The primary use of this capability is as a simple repository of important documents and links to be shared with other users. The C4I Suite provides Enterprise-wide and command-specific sharing capabilities.

4. Administration and Logistics. Recommendations for changes to this Order shall be submitted to the Commanding Officer, MCLB Albany (Attention: Mission Assurance Branch).

5. Command and Signal

a. Command. This Order is applicable to military and civilian personnel assigned or attached to MCLB Albany.

b. Signal. This Order is effective the date signed.

DONALD J. DAVIS

C4I Suite Mandatory Reporting Categories

	Reporting Categories	Responsible Staff	
		MA	LE
1	Any riot, demonstration, or disruption effort targeted at DoD and in a manner that directly threatens DoD personnel, infrastructure, resources, critical information or missions.	X	X
2	Any incident threatening DoD personnel, infrastructure, resources, critical information, or missions, when suspected or determined not to be an accident.	X	X
3	Illegal activities, initiated or sponsored by known or suspected domestic terrorists, extremists, supremacists, dissident groups, or criminal elements (organized criminal conspiracies or gangs as defined by law), directed against DoD personnel, infrastructure, resources, critical information, or missions.	X	X
4	The theft or acquisition of any chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) agents, munitions parts, precursors, or specialized equipment used in handling/processing of CBRNE materials or delivery systems, with the following reporting thresholds:		
	• Chemical materials. Any complete chemical munitions. Any amount of schedule 1, 2, or 3 toxic chemicals or their precursors as defined by the chemical weapons convention used in the manufacture of a chemical weapon agent or a high-yield explosive (civilian or military).	X	
	• Biological materials. Any biological weapon agent (civilian or military).	X	
	• Radiological materials. Any amount of radiological material capable of generating casualties (as opposed to medical radiological materials used routinely in small amounts).	X	
	• Nuclear materials. Any highly-enriched, weapons grade uranium or plutonium. Any nuclear weapons component.	X	
	• The theft or acquisition of any explosive precursor chemicals, munitions parts, or specialized equipment used in the handling/processing of improvised explosive devices with a DoD nexus.	X	
5	The theft of military arms, ammunitions or explosives (AA&E) that have not been rendered inert with the following reporting thresholds:		
	• Any missile, rocket, mine, mortar, or artillery shell.	X	X
	• Any machine gun or automatic weapon.	X	X
	• Any fragmentation, concussion, phosphorus, or high-explosive grenade.	X	X
	• Any explosives, detonation cord, or blasting caps.	X	X
	• Actual or attempted break-ins of weapons rooms or storage areas for AA&E.	X	X

6	Tactics, techniques, and procedures used by terrorists and homegrown extremists to include suspicious activities that may indicate pre-operational planning or targeting of DoD personnel, infrastructure, resources, critical information, or missions.	X	X
7	Non-specific threats to include plans, intentions, use, or potential use of false identities, statements, writings, or documents for facilitating illegal entry onto DoD facilities, including but not limited to unexplained loss, theft, or replication of badges (e.g., identification badges, access cards or badges, visitor passes, etc.) uniforms, vehicles, or government identification media.		X
8	Surveillance Activities: • Static surveillance. Persons loitering and observing entry/exit/delivery protocols, access controls, as well as photographing, videotaping, or sketching diagrams of DoD infrastructure or assets. • Mobile surveillance. Repeated vehicular drive-by or fly-over that may include videotaping or photographing DoD infrastructure, assets, perimeter security measures, or entry control points. • Specific surveillance. Surveillance or attempts to solicit information of a particular building, area, organization, or person on a DoD facility, to include access control and antiterrorism measures.		X X X
9	Elicitation, such as attempts to obtain protected, proprietary, business confidential, protected critical infrastructure information, or otherwise sensitive DoD information including the illegal acquisition of military expertise.	X	X
10	Tests or penetration of security or access control procedures at DoD facilities, such as attempts to probe security through elicitation, cyber exploitation, or other means.		X
11	Traffic barrier operation failure. Any malfunction, to include test malfunction, or incident malfunction, where traffic barriers or final denial devices do not function or operate as designed.		X
12	Suspicious attempts to gain employment at critical facilities, with security units or with outside vendors with access to critical DoD facilities, infrastructure or assets; attempts to recruit insiders to support/advance criminal activities planning or execution; information that identifies plans for deception, diversionary tactics, or planned breaches of security.	X	X
13	Any reported association or communication by a DoD affiliated person in support of a terrorist, extremist, supremacist, gang, or organized criminal organization.	X	X
14	Conspiracy or conduct of illegal acts against DoD, such as blocking DoD convoys.	X	X
15	Agenda-driven activities, or hate crimes, directed against DoD personnel, infrastructure, resources, or critical information with the intent of degrading or disrupting the DoD mission.	X	X

16	Threats, (voice, data, in person) plans or attempts to harm or kidnap, or other information bearing on the personal security of the President of the United States, other senior officials whose security is supported by DoD (e.g., airlift, bomb dog teams), or any combatant commander or other designated high risk personnel residing in/transiting the USNORTHCOM AOR.	X	X
17	Any other incident identified by the Commander, USNORTHCOM, particularly in the context of ongoing world events, to be of immediate concern to USNORTHCOM based on its nature, gravity, potential for adverse publicity, or potential consequences.	X	X
18	Mass notification (AtHoc or Mass Notification System) operation failure. Any non- connectivity or malfunction, where mass notification measures do not function or operate as designed.	X	X
19	Expressed or implied threat (voice, data, in person). A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.	X	X