**UNITED STATES MARINE CORPS**
MARINE CORPS BASE HAWAI'I
BOX 63002
KANEOHE BAY HAWAI'I 96863-3002

Canc: Jan 2026

MCBHBul 3070
CO
12 FEB 25

MARINE CORPS BASE HAWAI'I BULLETIN 3070

From: Commanding Officer
To: Distribution List

Subj: OPERATIONS SECURITY CRITICAL INFORMATION AND INDICATORS LIST

Ref: (a) MCO 3070.2A

Encl: (1) MCBH Critical Information and Indicators List (CIIL)

1. Purpose. The purpose of this bulletin is establishing the Critical Information and Indicators List (CIIL) for personnel assigned to Marine Corps Base Hawai'i(MCBH).

2. Background. Per the provisions of the reference, CIIL must be provided to MCBH personnel to establish unclassified information which is sensitive to include controlled unclassified information. This list does not include classified information, personal identifying information, or personal health information requiring specific safeguarding procedures.

3. Action. Information contained in the CIIL will be safeguarded by all members of MCBH. Identification of information reasonably believed to constitute an unapproved release of critical information or a critical indicator must be reported to the Security Office or Operations Security Program Manager immediately.

4. Operations Security (OPSEC). Prior to releasing documentation for public dissemination that is reasonably believed to constitute critical information or indicators, an OPSEC Review must be conducted by the MCBH OPSEC Program Manager (PM). The individual intending public dissemination must send an encrypted copy of all media intended for dissemination to the MCBH OPSEC PM no later than 7 days prior to intended dissemination, unless impracticable. The OPSEC PM will review the material for indicators of critical information. The MCBH OPSEC PM will issue concurrence in writing or a nonconcurrence memorandum identifying findings and recommendations for removal.

5. Applicability. This Bulletin is applicable to MCBH and subordinate commands and effective the date signed.

J. W. BEAVEN

DISTRIBUTION: A

# Marine Corps Base Hawaii
# Critical Information and Indicators List (CIIL)

The following list of Critical Information and Indicators requires OPSEC review before public dissemination or release. Public dissemination or release is the physical, oral, or digital release of information into the public domain where anyone can obtain the information.

Information. Critical information includes military activities, intentions, capabilities, or limitations that an adversary seeks to gain a military, political, diplomatic, economic, or technological advantage and can result in the degradation of mission accomplishment, loss of life, or damage to friendly resources.

Indicators. OPSEC indicators are defined as detectable actions and open-source information that can be interpreted or pieced together to allow an adversary to obtain critical or sensitive information while exposing vulnerabilities. The five types of indicators are:

**Signature** – characteristic that makes information identifiable (vehicle with unit markings)

**Association** – observations that relate information (different vehicles with same unit markings)

**Profile** – repetitive signatures and associations (unit only operates two types of vehicles)

**Contrast** – observable difference in a profile (unit now operating another vehicle type)

**Exposure** – duration, location, and timing of signatures creating a pattern (unit vehicles depart or return at same time over several days)

EXAMPLE:

1. **Type of Critical Information**. Brief description

a. Indicators (SAPCE) are not all-inclusive and provide the most common examples of critical information.

Critical Information and Indicators

1. **Personnel**. Information associated with command strength, readiness, access control, special assignments, and similar data.

    a. Leave requests, TDY/TAD status (S)
    b. Access rosters, Appointment orders (A)
    c. Unit readiness status (P)
    d. Deployment readiness schedules (C)
    e. Duty roster, work schedules (E)

2. **Intelligence**. Information associated with command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), security clearance, and similar data.

    a. Badges with clearance (S)
    b. Access procedures (A)
    c. Surveillance reports, inspection assessments, security breaches (P)
    d. Deviations from approved procedures, VIP visits (C)
    e. Intelligence reports (E)

3. **Operations**. Information associated with command and control (C2), airfield operations, standard operating procedures (SOPs), training, inspections, visits, and similar data.

    a. Organizational charts (S)
    b. Command relationships (A)
    c. Capabilities brief, Concept of Operation (P)
    d. Training status (C)
    e. Training schedules (E)

4. **Logistics**. Information associated with supply, equipment, motor transport, contracting, maintenance, construction, and similar data.

    a. Motor pool activities (S)
    b. Specialized equipment storage, Exterior labelling of storage boxes (A)
    c. Priority of requisitions, Pre-positioned stock (P)
    d. Transport requests, Deviations in support activity (C)
    e. Delivery schedules (E)

5. **Planning**. Information associated with land use, future operations, lessons learned, conferences, seminars, meetings, force design, force transformation, and similar data.

    a. Range requests (S)
    b. Patch Chart, Chiclet Chart (A)
    c. After Action Reports, Executive Summaries (P)
    d. Risk Assessments (C)
    e. Multi-year exercise plan (E)

6. **Communications**. Information associated with MCEN, system authorization, nodes, servers, infrastructure, distribution, and similar data.

    a. Call Signs, Contact Lists (S)
    b. Frequencies, Conference Call Codes (A)
    c. Test reports, Communication Status (COMSTAT) (P)
    d. Primary, Alternate, Contingency, Emergency (PACE) plans (C)
    e. Scheduled outages (E)

7. **Force Protection**. Information associated with Force Protection Conditions (FPCONs), Random Antiterrorism Measures (RAMs), crisis management, critical infrastructure, mission essential vulnerable areas (MEVAs), restricted areas, barrier plans, physical security, and similar data.

    a. FPCON Action Sets (S)
    b. Barrier resource application (A)
    c. Physical security deficiencies (P)
    d. Resource acquisitions beyond minimal requirements (C)
    e. RAMs schedule, Activation orders (E)

8. **Finance**. Information associated with pay, timecards, official travel, budgets, contracts, and similar data.

    a. Timecards (S)
    b. Pay issues, reduction in pay grade (A)
    c. Budget shortfalls, Excessive spending reports (P)
    d. Cancelled contracts, Denied funding requests (C)
    e. DTS authorizations (E)

9. **Law Enforcement & Emergency Services**. Information associated with incident response, casualties, displaced civilians, specialized equipment, detection, and similar data.

    a. Marking vehicles with specific function (S)
    b. Hours of operation for specialized functions (A)
    c. Indicating reduced response coverage areas (P)
    d. Additional equipment requirements or personnel (C)
    e. Special event support schedules (E)

10. **Geospatial Data**: Information associated with maps, diagrams, photos, layouts, labels, and other geographical data of installation facilities and infrastructure.

    a. Labeling unit buildings, construction drawings, utilities (S)
    b. Pictures of unit building, infrastructure, abnormal construction (A)
    c. Map of unit footprint, Design reports and summaries (P)
    d. Identifying structures by previous use “old communications building” (C)
    e. Including metadata such as unit POCs, capabilities, hours of operation, special designations (E)