DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND PACIFIC
HEADQUARTERS, UNITED STATES ARMY GARRISON DAEGU
OPC 305 BOX 23
APO AP 96218-9001

AMIM-DAO (1oo) 05 February 2026

MEMORANDUM FOR All Personnel Assigned or Attached to Area IV, Daegu Installation

SUBJECT: United States Army Garrison (USAG) Daegu Commander Policy Letter 26-02, Operations Security (OPSEC)

1. References:

a. AR 25-55, Freedom of Information Act Program, 19 Oct 20.

b. AR 360-1, The Army Public Affairs Program, 8 Oct 20.

c. AR 381-12, Threat Awareness and Reporting Program, 13 Jun 25.

d. AR 530-1, Operations Security, 26 Sep 14.

e. IMCOM Reg 525-2, Installation Management Command Protection Program, 1 Oct 23.

f. Army in Korea Regulation 530-1, Operations Security (OPSEC), 1 July 16.

2. This policy applies to USAG Daegu Soldiers/KATUSAs, DAC Employees, Contractors, Local National Employees, and Family Members.

3. OPSEC protects sensitive and/or critical information from adversary observation and collection in ways that traditional security programs cannot. While these programs, such as Information Assurance (IA), protects classified information, they cannot protect and safeguard all indicators. It also determines when that information may cease to be critical in the lifespan of an organization's specific operation.

4. OPSEC awareness and execution is crucial to USAG Daegu success. OPSEC is applicable to all personnel, missions and supporting activities on a daily basis. OPSEC denies adversaries information about friendly capabilities, activities, limitations, and intentions that adversaries need to make operational decisions. It applies to all USAG Daegu activities and is required during training, sustaining, preparing for, and conducting operations, exercises, tests or daily activities.

5. Securing classified information is well understood and enforced. However, everyone must understand that sensitive unclassified information needs protection and should be

denied to our adversaries. When small bits of information are fused together it reveals a larger picture. USAG-Daegu Critical Information List (CIL) is unclassified information that needs protecting from unauthorized disclosure. See your local OPSEC officer or the DPTMS to obtain a copy of the CIL.

6. USAG Daegu Soldiers/KATUSAs, DAC Employees, Contractors, Local National Employees, and Family Members, must protect both classified and sensitive unclassified information that, on potentially be exploited by our adversaries. We must make OPSEC a priority and integrate OPSEC practices into our daily activities.

7. The successful enforcement of OPSEC procedures can prevent serious injury and death of USAG Daegu members; damage to our key infrastructures; or loss of critical technological capabilities.

8. Punishment can occur if military personnel fail to comply with these orders, directives, or policies as violations of a lawful order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary or administrative measures.

9. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative or disciplinary actions.

10. Point of contact for this memorandum is the USAG Daegu, DPTMS OPSEC Officer, Ms. Catina Tomlinson at 763-6684.

NOLL.JEFFREY.D.1037656719 Digitally signed by NOLL.JEFFREY.D.1037656719 Date: 2026.04.21 15:32:49 +09'00'

2 Encls
1. USAG-D OPSEC Measures
2. USAG-D CIL Jul 25

JEFFREY D. NOLL
COL, IN
Commanding

USAG-Daegu General OPSEC Measures

1. Know the organization's critical information.

2. Implement OPSEC measures as ordered by the commander, director or individual in an equivalent position.

3. Receive a Newcomer OPSEC Orientation within 30 days of assignment to the unit.

4. Receive OPSEC Refresher briefings annually.

5. Know the answers to the following questions:

   a. What is my organization's critical information?
   b. What critical information am I personally responsible for protecting?
   c. How is the threat trying to acquire my critical information?
   d. What steps am I taking to protect my critical information?
   e. Who is my OPSEC Officer/Coordinator?

6. Avoid posting personal information on social networking sites or personal web sites which could compromise the safety or lives of DOD personnel. This includes personally identifiable information on Family, friends, and co-workers. Items to avoid posting on these sites include (but not limited to):

   a. Names
   b. Dates of birth
   c. Home addresses
   d. Social security numbers
   e. Family, biographies
   f. Photographs
   g. Personal schedules
   h. Group or unit rosters
   i. Official title
   j. Telephone number (personal)
   k. Organization charts (with names)
   l. Pay information
   m. Marital status
   n. Names, genders and number of Family members

USAG-Daegu Critical Information List Jul 2026

1. **Current, Ongoing and Future Operations Details**
   Examples: Mobilization, deployment schedules, stationing, logistical shortfalls, readiness levels, rosters

2. **Critical Infrastructure**
   Examples: Location, capabilities, weakness, airfields, communications, reports, plans, maintenance schedules, access control

3. **Force Protection**
   Examples: RAM measures, emergency response, new or emerging technology, access control, gaps, physical security

4. **Capabilities and Vulnerabilities**
   Examples: Purpose of COOP exercises, disaster plans, nodes, Contingency Plans for Emergency Situations

5. **Organizational Capabilities, Limitations and Vulnerabilities**
   Examples: Morale, inspection results, surveys, reductions

6. **General Officer and VIP Itineraries**
   Examples: Schedules, locations, special protective measures, visitors

7. **Budget and Resource Information**
   Examples: Allocation, prioritization, shortfalls, contract specifics

8. **Threat details to U.S. Forces, Agencies, Partner Nations**
   Examples: Assessment, government control, Coordination with Federal and Local Agencies on Intelligence Sharing

9. **Personally Identifiable Information (PII)**
   Examples: HIPPA, CUI, LE-Sensitive, hiring actions, alert roster

10. **Detailed Casualty, Damage or Incident Reports**
    Examples: SIR, Report of Survey,15-6 results