UNITED STATES FORCES KOREA INSTRUCTION

FKJ3 USFKI 3213.01
DISTRIBUTION: A, B 6 January 2022

USFK Operation Security (OPSEC)

References: See Enclosure B.

1. Purpose. This directive establishes policy and assign responsibilities governing United States Forces Korea's (USFK) OPSEC program, incorporating the requirements of CJCSI 3213.01D Joint Operations Security and USPACOMINST 0302.1.

2. Applicability. This directive applies to Department of Defense (DoD) and Korean National (KN) civilian employees, invited contractors, technical representatives, and all others supporting USFK operations.

3. Policy. It is USFK policy that missions, functions, programs, and activities shall be protected by an OPSEC program that implements DoD Manual 5205.02. The level of OPSEC to apply is dependent on the threat, vulnerability, and risk to the assigned mission, function, program, or activity, and available resources.

4. Releasability. Cleared for public release.

5. Effective Date. This directive is in effect until superseded or cancelled.

6. Proponent. USFK OPSEC proponent is J39 Information Operations, OPSEC Program Manager at DSN 315-755-4065

(Original Signed)
BRAD SULLIVAN
Major General, USAF
Chief of Staff

Enclosures
A--USFK Critical Information List
B--References

(INTENTIONALLY BLANK)

ENCLOSURE A

USFK CRITICAL INFORMATION LIST

Critical information deals with specific facts about military intentions, capabilities, operations or activities. If an adversary knew this detailed information, our mission and personnel safety could be jeopardized. Critical information must be protected to ensure an adversary doesn't gain a significant advantage the following is the USFK critical information list (CIL):

1. US and ROK VIP movement, itineraries, or schedules.

2. Force composition, operations, or missions.

    a. Schedules or timelines for operations and training events.

    b. Damage Reports and force casualties.

    c. Courses of actions (COAs) or proposed COAs.

3. Unit movements or intended movements and locations.

4. Movements and locations of major logistics caches or resupply operations.

5. Presence or employment of new or improved technology.

6. Information on USFK capabilities, vulnerabilities, and limitations such as:

    a. Weapons systems.

    b. Physical security and force protection of military installations.

    c. Logistics support for current and future operations.

7. Estimates of the effectiveness of operations.

8. Collection capabilities, purposes, and intent.

9. Communications and automated information system.

    a. User IDs, password, call-signs, and frequencies.

    b. Equipment limitations, capabilities, and dependencies.

    c. Details of intrusion into friendly network systems.

(INTENTIONALLY BLANK)

ENCLOSURE B

REFERENCES

a. DoDM 5205.02, “DoD Operations Security (OPSEC) Program Manual”, 3 November, 2008

b. DoDI 5220.22, “National Industrial Security Program (NISP)”, 18 March 2011

c. CJCSI 3213.01D, “Joint Operations Security”, 7 May 2012

d. USPACOMINST 0302.1, “Operation Security (OPSEC)”, 22 July 2016.

(INTENTIONALLY BLANK)