DEPARTMENT OF THE ARMY
HEADQUARTERS III CORPS AND FORT HOOD
BUILDING 1001 761st TANK BATTALION AVENUE
FORT HOOD, TEXAS 76544-5000

COMMANDING GENERAL'S POLICY LETTER #15

AFZF-CG

OCT 31 2022

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Operations Security (OPSEC)

1. REFERENCE. Army Regulation (AR) 530-1 Operations Security, dated 26 September 2014.

2. APPLICABILITY. This policy applies to all III Armored Corps service members, civilian personnel, and contractors assigned to and under the operational control of III Armored Corps.

3. STATEMENTS OF PURPOSE AND NECESSITY:

a. Combat capability increasingly depends on gaining and maintaining information superiority. All aspects of raising, equipping, training, deploying, employing, and sustaining forces affect this superiority. Failure to protect information can result in serious injury or death to our personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies, and mission failure.

b. Critical Information List (CIL) are facts and sensitive information about capabilities, activities, limitations, vulnerabilities, and intentions that help adversaries to plan against us, or interfere with our mission accomplishment (III Armored Corps CIL is enclosed). OPSEC protects critical information from adversary observation and collection by identifying indicators that might reveal critical information, and then developing measures to eliminate, reduce, or conceal those indicators.

4. POLICY. AR 530-1, dated 26 September 2014, and the III Armored Corps OPSEC Program require commanders at all levels to ensure their units or organizations integrate and implement OPSEC measures to protect critical information. Every Army organization possesses information that ultimately affects the ability of US forces to accomplish missions. Every organization must identify and protect information that an adversary could use against the US or other friendly forces. Every unit for which the commander or director is a Lieutenant Colonel, or Civilian equivalent, or higher, will establish and maintain a documented OPSEC Program and appoint in writing their OPSEC Level II trained primary and alternate OPSEC Officer. All III Armored Corps service members, civilian personnel and all contracted or other personnel otherwise assigned to and under the operational control of III Armored Corps will:

a. Know what their organization considers to be critical information, where it is located, who is responsible for it, how to protect it, and why it needs to be protected.

b. Protect from disclosure any Critical Information (CI) to which they have personal access to include CI from other branches of service, foreign governments, and contractor proprietary information.

c. Not take pictures of military assets or share photographs displaying CI.

d. Not Post videos, pictures, or information on social media while in uniform and/or conducting training and/or operations without approval from the unit's public affairs officer.

e. Not publicly reference, discuss, share, or confirm CI that has already been compromised as this provides further unnecessary exposure of the compromised information and may serve to validate it.

f. Actively encourage others, including Family members and Family Readiness Groups (FRGs), to protect CI.

g. Encrypt all emails that include sensitive information or CI on the unclassified network.

h. Comply with command policy/direction as well as existing regulations prior to publishing or posting sensitive information that may be released into the public domain.

i. Report attempts by unauthorized personnel to solicit CI per AR 381-12.

j. Burn or shred CI that is no longer needed per the standards in AR 380-5 and AR 25-400-2, in order to prevent the inadvertent disclosure and reconstruction of this material.

k. Remove access badges before leaving the building where the badge is required.

5. PUNITIVE ORDER. This policy is punitive and is intended to be a lawful general order and regulation within the meaning of Article 92, UCMJ, and 18 USC 1382. Violations of this policy may result in punitive action under the UCMJ, adverse administrative action, or both. Personnel not subject to the UCMJ who fail to protect sensitive and/or critical information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

6. This policy memorandum supersedes the Operations Safety memorandum dated 25 July 2019 and will remain in effect until superseded or rescinded.

SEAN C. BERNABE
Lieutenant General, USA
Commanding

Encl
1. Critical Information List

DISTRIBUTION:
IAW FH FORM 1853: A

Enclosure 1 to Commanding General's Policy Letter #15-Operations Security: Fort Hood Critical Information List

Fort Hood

Critical Information List

Operations Security protects sensitive, but generally unclassified information that is critical to our mission. Critical information consists of *specific* facts about our *capabilities, activities, limitations, and intentions* (CALI). The critical information is so vital to the mission that if the adversary obtains it, correctly analyzes it, and acts upon it, the compromise could prevent or seriously degrade mission success. The Critical information List (CIL) documents an organization's critical information that should be protected. The III Armored Corps and Fort Hood, TX CIL is as follows:

- **S**ensitive Reports: reports containing sensitive and / or personally identifiable information (PII) or information pertaining to mission readiness such as blotters, battle damage assessments, recall rosters, manning documents, etc.

- **E**merging Tactics, Techniques, and Procedures (TTP): newly administered TTPs to improve mission effectiveness such as ways to avoid or detect IEDs, convoy protection methods, etc.

- **N**etwork & Communications Related: call signs, frequencies, passwords, Automated Information Systems (AIS) protection (types used, measures, and procedures), changes in message volume, etc.

- **S**ecurity Plans and Procedures: Random Antiterrorism Measures, shift change for guards, changes in FPCON, DEFCON, or INFOCON, etc.

- **I**ntelligence, Surveillance, and Reconnaissance (ISR): intelligence resources, collection techniques, ongoing operations and goals, counterintelligence operations, etc.

- **T**roop Movements & Travel: deployment/ redeployment times, locations, itineraries, ports, routes, embarkation points, VIP travel, TOY orders, leave for large groups or entire units, emergency recall of personnel, etc.

- **I**nformation Pertaining to Current *I* FUOPS: deployment plans, exercises, scope of operations, planning details, specific Courses of Action (COAs) for forces, Rules of Engagement/Use of Force (ROE/ RUF), Military Information Support Operations (MISO) and Military Deception

(MILDEC) operations, Special Access Programs SAP elements in contracts, Personally Identifiable Information (PII)

- **V**ulnerabilities: a condition that allows the adversary time to observe, orient, decide and act against us in areas such as critical infrastructure, building schematics that show security weaknesses, physical security shortfalls, etc.

- **E**quipment Specifications and Limitations: shortfalls, vehicle schematics, vehicle battle damage assessments, weapons systems, research and development (R&D) projects,electronic systems, software used in new systems, Force Modernization efforts, etc.

1. The above list is maintained by III Armored Corps G39 on behalf of the CofS and all subordinateelements to III Armored Corps and Fort Hood.