



DEPARTMENT OF THE ARMY
UNITED STATES ARMY EUROPE
UNIT 29351
APO AE 09014-9351

AEOP-PT-AT


7 January 2020

MEMORANDUM FOR All USAREUR Military and Civilian Personnel

SUBJECT: USAREUR Critical Information List (AE Cmd Memo 2020-001)

1. This memorandum supersedes memorandum, USAREUR, AEOP-PT, 12 April 2018, subject: USAREUR Critical Information List (CIL) (AE Cmd Memo 2018-033).
2. We operate in an environment where information is shared through a variety of different venues at near instantaneous speeds and is accessible to various actors around the globe. While the modern communications environment allows for unprecedented opportunities to share and access information, it also presents challenges to USAREUR operations security (OPSEC) efforts.
3. The CIL, also known as Essential Elements of Friendly Information, consists of classified and unclassified elements of information and provides answers to key questions that our adversaries are likely to ask about our capabilities, plans, procedures, and intentions. Hostile intelligence organizations or other adversaries can combine seemingly harmless bits of information to form a more complete picture of our capabilities, activities, and plans. Adversaries can use this information to harm friendly personnel or hinder operations.
4. The [enclosed USAREUR CIL](#) comprises information that is vital to the USAREUR mission. Army in Europe personnel, whether military, civilian, or contractor, will use OPSEC measures and countermeasures to protect this critical information.
5. CILs are adapted to various operations and specific units. All USAREUR subordinate units are required to develop a CIL specific to their mission. These subordinate CILs must include all elements of the USAREUR CIL.
6. The POC for this memorandum is the USAREUR OPSEC Program Manager at military 314-537-3692 or 314-537-3132.

Encl


CHRISTOPHER G. CAVOLI
Lieutenant General, USA
Commanding

USAREUR Critical Information List

- 1. Location and Capabilities of Key Assets and Weapon Systems:** Capabilities identified by operations plans, contingency plans, or missions, for which maintaining essential secrecy is necessary for executing the commander's intent, and the conditions affecting their readiness, deployment, and employment.
- 2. Details and Scope of Current and Future Operational Activities Until Authorized for Public Release by the Office of Public Affairs, HQ USAREUR, or Headquarters, Department of the Army:** Missions, objectives, dates, times, and strategies; movements and itineraries of general officers and distinguished visitors; force capabilities and limitations; rosters; movement of forces; current and emerging tactics, techniques, and procedures.
- 3. Personally Identifiable Information (PII):** This also includes PII of coalition partners and foreign nationals who are supporting operations.
- 4. Security Plans and Procedures:** Specifics about access control, physical-security capabilities, force-protection assets, random antiterrorism measures, schedules, installation arming locations, unpublicized special events (for example, high-school graduations), unpublicized off-installation movements, building evacuation plans and procedures, and emergency action drills.
- 5. Logistics Information:** Manifests; speed of deployment and redeployment of forces; contracting and funding data; deployment of special equipment; equipment-readiness rates; supply status; pertinent ground, air, and sea lines of communications; locations and capabilities of critical storage depots, ports, and airfields.
- 6. Communications Involved With or in Support of Operations:** Communications architecture and diagrams; network and system configurations; network identifiers and call signs; personal identification numbers and passwords; frequencies; information network vulnerabilities or deficiencies, capabilities, restrictions, and limitations; IT contingency plans; disaster recovery plans; restoration procedures, and special equipment.
- 7. Intelligence, Surveillance, and Reconnaissance Asset Support:** Collection techniques, capabilities, or limitations.
- 8. Real-Property Information:** Blueprints; detailed diagrams; facility-utilization studies; floorplans; maps or photos of base or camp layouts; and geospatial data.
- 9. Defense Critical Infrastructure:** May include, but is not limited to the following: Specifics about electric power systems; communications nodes and lines; automations nodes and lines; data centers; railheads and rail lines; airfields; ammunition storage sites; hospitals and medical facilities; ports, roads, and intersections; fuel points; POL tank farms; headquarters facilities; intelligence facilities; fire departments; operations facilities; maintenance facilities; and supervisory control, data acquisition, and industrial control systems.