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

AEIM-I 28 October 2016

MEMORANDUM FOR All Army in Europe Commanders

SUBJECT: USAREUR Instructions for the Use of Mobile Devices and Laptops When Traveling to Turkey and the Ukraine (AE Cmd Memo 2016-056)

1. References:

a. USEUCOM GENADMIN message, date-time group (DTG): 261200Z May 16, subject: USEUCOM GENADMIN Assigning United States Army Europe (USAREUR) as Approval Authority for Department of Defense (DOD) Travel and Deployments to and Within the Ukraine.

b. USAREUR Message # 1606009, DTG: 031723Z Jun 16, subject: FRAGORD 7 (Ukraine Travel and Deployment Approval) to USAREUR OPORD 0038-16 (FY16–FY17 Baseline FP Posture) (contents FOUO).

c. USAREUR Deployment Compliance Scanning Tactics, Techniques, and Procedures (TTP) at *https://intranet.eur.army.mil/hq/iassure/IAVM/Pages/default.aspx*.

2. Foreign intelligence services have the capability to disrupt our critical information technology (IT) systems and services by deploying malware on mobile devices (for example, smartphones, tablets) and computers, resulting in sensitive information being compromised.

3. Effective immediately, commanders will ensure that all travelers to Turkey and the Ukraine comply with the following security measures:

a. Before traveling, travelers will—

(1) Coordinate predeployment scans of their laptops with their information systems security manager (ISSM).

(2) Notify their telephone control officer (TCO) of any smartphones and tablets that will be deployed.

b. On their return, travelers will—

(1) Contact their ISSM to coordinate postdeployment scans of their laptops.

AEIM-I
SUBJECT: USAREUR Instructions for the Use of Mobile Devices and Laptops When Traveling to Turkey and the Ukraine (AE Cmd Memo 2016-056)

(2) Have their TCO restore their mobile devices to factory settings.

(3) Not use their laptops, smartphones, and tablets until postdeployment measures are completed.

4. Units will send the scan results to the USAREUR G6 in accordance with reference 1c.

5. This is commander's business. Commanders are responsible and accountable for security controls for deployed devices to mitigate the risk to our critical network infrastructure. I expect all commanders to make prudent risk-based decisions to increase the consistency, effectiveness, and timeliness of our security controls.

6. The POC is the USAREUR Cybersecurity Program Manager at military 314-537-6204.

TIMOTHY P. MCGUIRE
Major General, USA
Deputy Commanding General