



HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131-0400

ECCS

21 October 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: USEUCOM Policy Memorandum 03-06 (USEUCOM Portable Computing Device Policy)

1. **References.**

- a. USEUCOM Directive 25-4, "USEUCOM Policy Guidance for Use of Portable Electronic Devices within Sensitive Compartmented Information Facilities.", 22 Oct 2002
- b. USEUCOM Directive 25-5, Information Assurance, 1 July 2002

2. **Summary.**

- a. Recent computer security incidents and events within the USEUCOM AOR highlight the need to ensure adherence to rigorous security practices for portable computing devices.
- b. This memorandum establishes basic guidelines and standards for use of portable computing devices that connect to DoD unclassified and classified networks within the USEUCOM AOR. Examples of portable computing devices include but are not limited to laptops, notebooks, handheld computing devices (e.g. Palm Pilot, BlackBerry, iPaq, etc.) and any other portable computing devices that store, transmit or process data.
- c. HQ USEUCOM, Service Components and supporting elements are directed to develop clear implementation procedures for security management of portable computing devices that connect to DoD networks within the USEUCOM AOR.

3. **Applicability.** This Policy Memorandum applies to all elements within USEUCOM to include HQ USEUCOM, USAREUR, USAFE, NAVEUR, MARFOREUR, SOCEUR, USFORAZ, ICEDEFOR, all USEUCOM-directed Joint Task Forces (JTF) and Combined Joint Task Forces (CJTF), as well as COCOM-supporting elements operating in the USEUCOM Area of Responsibility (AOR) regardless of administrative chain of command (hereafter referred to as "Components and supporting elements"). This policy specifically addresses the use of portable computing devices used to store, transmit or process government unclassified or classified data. **This policy does not apply to laptops or other portable electronic devices used with Sensitive Compartmented Information Facilities (SCIFs). For policy on the use of portable electronic devices within SCIFs, see reference a.**

4. **Policy.** It is USEUCOM policy that Components and supporting elements shall develop implementation procedures addressing the security of portable computing devices.

a. Component and supporting element policy will address initial connection and/or subsequent re-connection to networks in the USEUCOM AOR. Specifically the guidance and procedures will address:

(1) Compliance with a secure configuration baseline Operating System (OS). Components and supporting elements shall develop secure configuration baseline guidance for all devices which connect to unclassified and classified networks.

(2) Compliance with all Information Assurance Vulnerability Alerts (IAVAs) as required by DoD and USEUCOM policy. Components and supporting elements are required to implement USEUCOM-directed IAVAs IAW reference b.

(3) Compliance with current AntiVirus capabilities, signatures and definitions.

b. This policy memorandum is supplemental to existing DoD and USEUCOM policies, the DISN Connection Approval Process and the DoD Information Technology Security Certification and Accreditation Process. This policy will be included in future revisions of ED 25-5.

5. **POC.** POC for this policy is USEUCOM J62, DSN 430-8225.

FOR THE COMMANDER

OFFICIAL:

JOHN B. SYLVESTER
LTG, USA
Chief of Staff

DANIEL A. FINLEY
MAJ, USA
Adjutant General

DISTRIBUTION:

P