



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

May 3, 2007

INSPECTOR GENERAL INSTRUCTION 7950.3

MOBILE COMPUTING DEVICES

FOREWORD

This Instruction establishes the Department of Defense Office of Inspector General Mobile Computing Device policy. Policies and responsibilities regarding the use of Mobile Computing Devices, especially in secure or sensitive areas, are defined along with possible threats of using Mobile Computing Devices.

This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

A handwritten signature in black ink, appearing to read "SD Wilson".

Stephen D. Wilson
Assistant Inspector General for
Administration and Management

2 Appendices

A. **Purpose.** This Instruction establishes the Department of Defense Office of Inspector General (DoD OIG) Mobile Computing Device policy.

B. **References.** See Appendix A.

C. **Cancellation.** This Instruction supersedes IGDINST 7950.3, *Mobile Computing Devices*, April 5, 2001.

D. **Applicability and Scope**

1. This Instruction applies to the Offices of Inspector General, the Deputy Inspectors General, the Assistant Inspectors General who report to the Inspector General, the General Counsel, and the Director, Equal Employment Opportunity, hereafter referred to collectively as the OIG Components.

2. This Instruction applies to all mobile computing devices, whether Government issued or personally owned.

E. **Definitions.** See Appendix B.

F. **Background**

1. Mobile computing devices may include features such as infrared, radio frequency, and telephone modem communications capabilities. These same features allow easy connectivity between a mobile computing device and other devices for performing data exchanges and along with their expanded memory and processing ability, create new vulnerabilities for compromise. Attempts to temporarily disable these features by external means may not actually be solutions and, in some cases, may even enhance the associated vulnerabilities. The transmission of information between a wireless device and an Internet server is no different than a radio broadcast. Anyone with a receiver can eavesdrop. Wireless messages can be intercepted or tampered with in ways not possible with wired connections.

2. Since most, if not all, units are capable of both sending and receiving without indication to the user, this feature poses a high security risk.

3. When mobile computing devices are permitted within the OIG an enormous amount of trust is placed on the user to provide physical security for the device. Contained within the mobile computing device are all the components needed for a remotely activated surveillance device.

G. **Policy**

1. Mobile computing devices other than those pre-approved by ISD are not standard hardware or software, as specified in reference (a).

2. The OIG shall not compromise sensitive data, as defined in reference (b) via mobile computing devices, which may be referred to as personal digital assistants, palm tops, hand-held computers and workstations, web based enhanced cell phones, two-way pagers, and wireless e-mail devices. Classified data processing shall be performed only on accredited, classified systems.

3. Mobile computing devices shall not be used in areas where classified material is processed or discussed.

4. Users should not attempt to block sending and receiving features using any method that has not been approved by the Designated Approving Authority (DAA).

5. Since these devices may be used as a tool for sending e-mail, managing tasks, calendars, and staying in virtual constant contact with the OIG an increased potential exists for compromise of sensitive data. It is the responsibility of employees to ensure that their use of such devices does not lead to loss or exposure of information.

6. Appropriate physical security guidelines and procedures, as discussed in reference (b), are of paramount importance. The risk of compromising classified or sensitive information, resulting from users losing their mobile computing devices is considered high. If an adversary gained access to the mobile computing device for as little as 30 minutes, it could be reconfigured to collect, process, store, and retransmit classified or sensitive data from within the secure space. Users are strongly cautioned to protect their mobile computing devices during transit and report any suspicious activity involving their devices to the Office of Security and the Information Systems Directorate (ISD).

7. Mobile computing devices shall not be taken into any Sensitive Compartmented Information Facility (SCIF), a Special Access Program (SAP) facility, or a Special Access Required (SAR) facility.

8. Mobile computing devices can transmit computer viruses if their contents are uploaded to the OIG computers. Therefore, only mobile computing devices, designated as the OIG standard, and the associated OIG standard software that permits uploading will be loaded on the OIG computers. The connection of authorized, non-standard mobile computing devices is only on an exception basis and must be approved by ISD prior to connection and installation. Unauthorized mobile computing devices must not be connected and installed on OIG computers.

9. E-mail messages, like all electronic documents, may be considered agency records and are subject to the provisions of references (c), (d) and (e).

10. Users may not use unofficial e-mail services for official business without the express permission of the ISD.

11. Failure to adhere to the provisions of this Instruction may result in termination of access to all OIG supported local area networks and in other disciplinary and legal penalties, as appropriate.

12. Government owned mobile computing devices shall be procured in accordance with reference (f).

13. Only OIG procured third party Internet services subscriptions will be permitted on Government mobile computing devices.

H. Responsibilities

1. The **Inspector General** shall designate the DAA.

2. The **DAA** shall decide on accepting the security safeguards prescribed for mobile computing devices.

3. The **OIG Component Heads** shall ensure that the provisions of this Instruction and references (a) through (f) are implemented.

4. The **Human Capital Advisory Services (HCAS)** shall advise and assist management on appropriate administrative action if misuse occurs.

5. The **Information Systems Directorate (ISD)** shall load software to enable uploading of information from mobile security devices only on an exception basis.

6. The **Administration and Logistics Services Directorate (ALSD)** shall assist and advise when e-mail messages constitute records subject to the provisions of reference (c).

7. **Users** shall:

a. Not use mobile computing devices in areas where classified material is processed or discussed.

b. Not take mobile computing devices into a SCIF or SAP/SAR facilities.

c. Keep in mind that e-mail is subject to the provisions of references (c), (d), and (e).

d. Not use unofficial e-mail services for official business without the express permission of the ISD.

e. Not upload information stored on a mobile computing device into the OIG environment without the express permission of the ISD.

f. Refrain from any practices that might jeopardize, compromise, or render useless any OIG data, system or network.

g. Be individually responsible and liable for any disclosures of sensitive information if the employee sends such information through a mobile computing device.

h. Not send secure, sensitive, classified, or potentially compromising information through a mobile computing device unless approved by the DAA. All classified data transfers shall be performed only on accredited, classified systems. Information subject to references (d) and (e) shall be appropriately protected if transmitted electronically.

i. Maintain physical security of mobile computing devices at all times.

j. Not access the Internet or e-mail through the mobile computing device while it is connected to the computer (e.g., the device is in a cradle from which a cable runs to the computer.) This provision applies even if software to enable uploading of information from mobile computing devices has been loaded by the ISD, on an exception basis.

**APPENDIX A
REFERENCES**

- a. IGDINST 7950.2, *Computer Hardware and Software Management Program*, May 3, 2007
- b. IGDINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000
- c. IGDINST 5015.2, *Records Management Program*, May 3, 2007
- d. DoD Directive 5400.7, *DoD FOIA Program*, May 11, 2006
- e. DoD 5400.11-R, *DoD Privacy Program*, May 11, 2006
- f. IGDINST 7950.1, *Acquisition of Information Technology Resources*, May 3, 2007

APPENDIX B DEFINITIONS

1. **Designated Approving Authority (DAA)** is the official, appointed by the Inspector General, who has the authority to decide on accepting the security safeguards prescribed for an information system or that official who may be responsible for issuing an accreditation statement that records the decision to accept these standards. The DAA is currently the Director of Information Systems.
2. **Electronic Mail (e-mail).** A means of communication that uses computer-to-computer data transfer technology, normally as textual messages or attached files.
3. **Mobile Computing Device.** Electronics that have self-contained processing units, contain wireless telecommunications capabilities and are easily transportable. The definition includes, but is not limited to, equipment that may be referred to as personal digital assistants, palm tops, hand-held computers and workstations, web based enhanced cell phones, two-way pagers, and wireless e-mail devices
4. **OIG Environment.** Any computer, media, or network used by the OIG.
5. **User** is a person with authorized access to OIG computers, information systems, and/or information technology resources