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

May 3, 2007

INSPECTOR GENERAL INSTRUCTION 7920.5

SMALL COMPUTER USE

FOREWORD

This Instruction updates the Department of Defense Office of Inspector General Small Computer Use Program. Instructions and policies for using computers and other information technology resources are defined as well as procedures and responsibilities.

This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

for Marilynn M. Poladeck
Stephen D. Wilson
Assistant Inspector General for
Administration and Management

2 Appendices – a/s

A. Purpose. This Instruction updates the Department of Defense Office of Inspector General (DoD OIG) Small Computer Use Program.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDINST 7920.5, *Small Computer Use*, August 28, 2002.

D. Applicability

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 small computers and mobile computing devices as defined in reference (a) whether or not they are part of a network.

E. Definitions. See Appendix B.

F. Policy

1. Small computers and the information produced on them shall be protected vigorously from loss, misuse, and damage.

2. The OIG shall comply with the terms and conditions for commercial software use, including copyright and license agreements.

3. Government office equipment, including small computers, shall be used only for official purposes, except as specifically authorized in this Instruction. Users are permitted limited appropriate use of government office equipment for personal use, if the use does not interfere with official business and involves minimal additional expense to the government. This limited appropriate personal use of government office equipment shall take place during the users non-work time. This privilege to use government office equipment for non-government purposes may be revoked or limited at any time. This personal use shall not result in loss of user productivity, interference with official duties, or increase the vulnerability of the infrastructure and data contained. Inappropriate personal use is prohibited. Please see Appendix B for clarification of what constitutes inappropriate personal use. Moreover, such use shall incur only minimal additional expense to the government in areas such as:

a. Communications infrastructure costs; e.g., telecommunications traffic.

b. General wear and tear on equipment.

c. Data storage on storage devices.

d. Consumption of supplies; e.g., recordable optical disks, printer paper.

e. Transmission impacts with moderate electronic mail (e-mail) message sizes, such as e-mails with attachments smaller than 5 megabytes.

4. This policy in no way limits user use of government office equipment, including small computers, for official activities.

5. It is the responsibility of users to ensure that their personal use of government office equipment is not interpreted falsely to represent the agency. If there is an expectation of such an interpretation, a disclaimer shall be used, such as, "The contents of this message are mine personally and do not reflect any position of the government or my agency."

6. Users do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time, including accessing the Internet or using e-mail. To the extent that users wish that their private activities remain private, they shall avoid using office equipment such as the computer, Internet, or e-mail. By using government office equipment, users imply their consent to disclosing the contents of any files or information maintained or passed through government office equipment. By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of government small computers is made with the understanding that such use is generally not secure, private, or anonymous.

7. The OIG reserves the right to monitor all small computer use for the performance of operation, maintenance, auditing, security, or investigative functions. Further monitoring is used to enforce policies regarding official use and harassment and to access information when a user is not available. The Chief Information Officer (CIO) shall provide authorization for this monitoring.

8. Inappropriate personal use of small computers could result in loss of use or limitations on use of the equipment, disciplinary or adverse action, criminal penalties, and/or the user being held financially liable for the cost of the improper use in accordance with reference (b).

9. Users are specifically prohibited from using government office equipment to maintain or support a personal private business, or to assist relatives, friends, or other persons in such activities or for personal gain.

10. Access to some OIG systems, such as desktops and internet-based applications, is password controlled. Access to parts of other OIG systems is controlled administratively. Unauthorized access or attempts to access controlled systems or areas prohibited or restricted from use, either explicitly or implicitly, is considered misuse of information resources.

11. The connection, installation, or use of unauthorized hardware and/or software is prohibited on OIG computers. Components with a mission need to connect, install, and use unauthorized hardware and/or software, must provide requirement documentation, obtain an Information Systems Directorate (ISD) review, and receive written approval from the Designated Approval Authority (DAA) prior to connecting, installing, or using the unauthorized hardware and software. If approved by the DAA, the hardware and/or software become authorized.

12. The use of authorized non-standard hardware or software is a component level management decision and not supported by the ISD. If the ISD determines that non-standard hardware or software is causing a malfunction of standard hardware or software, the ISD reserves the right to return the user to the standard configuration.

13. In accordance with reference (c), privately owned hardware and/or software to include Portable Desktop Assistances (PDAs) or other mobile computing devices may not be connected to and installed on the OIG systems.

G. Responsibilities

1. The **CIO** shall:

a. Approve for the OIG policies implementing laws and guidelines on small computer management.

b. Provide leadership to manage small computers within the OIG.

c. Oversee the promulgation of policies and guidance to ensure the most effective, efficient use of small computers.

2. The **Designated Approving Authority (DAA)** shall:

a. Accept the security safeguards prescribed for access to the Internet and issue an accreditation statement that records the decision to accept those standards.

b. Provide written authorization for hardware and/or software.

3. The **ISD** shall:

a. Provide approved hardware, software, telecommunications, and other information resources to ensure the efficient, effective use of small computer systems.

b. Develop small computer policies, standards, and procedures.

c. Ensure compliance with applicable laws, guidelines, regulations, and standards, both internal and external. This includes, but is not limited to, public laws and the OIG, the General Services Administration (GSA), and the Office of Management and Budget (OMB) publications.

d. Manage small computer acquisition, maintenance, and support.

e. Provide user support, as defined in Appendix B.

f. Administer user identification or authentication mechanisms for those information systems under ISD control.

g. Provide advice and assistance to systems sponsors for those information systems not under ISD control.

4. The **Office of Security (OS)** shall:

a. Develop small computer security policies, standards, and procedures.

b. Ensure small computer use complies with applicable security laws, guidelines, regulations, and standards, both internal and external. That includes, but is not limited to, public laws and the OIG, the Defense Intelligence Agency, and the OMB publications.

c. Perform the duties delegated by the DAA.

d. Advise and assist management on appropriate administrative action(s) if misuse occurs.

e. Review unauthorized hardware and/or software and provide a recommendation to the DAA for approval or declination as authorized hardware and/or software.

5. The **User** shall:

a. Operate small computers within established laws, procedures, and guidelines. This includes, but is not limited to, public laws and the OIG, the GSA, and the OMB publications.

b. Notify his or her supervisor and the ISD, of every occurrence of loss, significant misuse, or significant damage to small computers and their contents.

c. Ensure the accuracy and integrity of data processed and transmitted.

d. Refrain from any inappropriate personal uses.

e. Refrain from altering the configuration of small computers following delivery or repair by the ISD or authorized contractors. Such tampering with hardware (e.g. removal of drives, memory, and/or circuit boards) may subject the user to administrative penalties in accordance with reference (b).

f. Refrain from connecting, installing, or using unauthorized hardware and/or software on OIG systems.

g. Submit requirements documentation and seek the ISD review, and the DAA approval for mission required unauthorized hardware and/or software.

h. Refrain from using privately owned software, hardware, PDAs, or mobile computing devices to access the OIG systems.

i. Not attempt to disable automatic virus scans. Ultimate responsibility for keeping small computers virus free remains with the user.

6. **Supervisors** shall:

a. Ensure employees are informed of OIG policies on small computer use and take every reasonable step to minimize waste and prevent misuse of information resources.

b. Designate responsible custodians for all components of information systems in their physical areas.

c. Develop procedures to ensure the effective, secure operation of information systems in their mission areas, to include ensuring that:

(1) All users protect information and information resources.

(2) All software used in his or her area is properly inventoried.

(3) All reasonable steps are taken to prevent infection of systems with viruses.

(4) All users refrain from any tampering or modifying hardware following delivery or repair by the ISD, or authorized contractors.

(5) All users make only authorized use of systems.

(6) All software-licensing agreements are enforced.

d. Communicate to all users their decisions regarding the authorized uses of communication systems and non-standard software and hardware.

e. Initiate or take appropriate disciplinary action against users who violate this Instruction, in accordance with reference (b), as appropriate.

H. Procedures

1. **Protection of Information.** Since the information stored in, and processed by, small computers frequently is more valuable than the computer itself, users shall take steps to preserve its integrity and protect it from infection by malware. Ultimate responsibility for keeping small computers malware free remains with the user. Users shall be alert for anything that is unexpected or may indicate a virus. Users shall consult with the Technical Support Center in these situations. References (d) and (e) provide additional precautions.

a. Storage media shall be protected and labeled commensurate with the sensitivity or classification level of the information to which they have been exposed. This includes information subject to the Privacy Act and information designated as “For Official Use Only” (FOUO). Data

deletion commands do not purge storage media of data. Although the user has deleted the file name, the data may still be accessible. As a minimum, if diskettes have ever been exposed to sensitive data, they shall be placed out of sight to avoid viewing of or tampering with data.

b. The user shall position information resources away from windows, open doorways, and other viewing areas to discourage theft and prevent disclosure of data to unauthorized persons.

c. Users shall duplicate or back up mission critical information and files that have taken significant time to create and store them separately from the original.

d. If the user introduces any authorized hardware and/or software into the OIG environment, that is not the OIG standard hardware or software, the user is responsible for it. This includes any effect that it may have on the operation of standard hardware and software, as defined in reference (f). Even virus free information resources may cause conflicts. If the ISD determines that non-standard hardware or software is causing a malfunction of standard hardware or software, the ISD reserves the right to return the user to the standard configuration. The ISD shall not assume responsibility for any functionality or data lost by return to the standard configuration.

e. Malware can be spread through e-mail, removable storage media, and the Internet. Therefore, there is a significant risk in opening e-mail attachments or downloading or using programs from the Internet. Ultimate responsibility for keeping small computers virus free remains with the user. Users shall exercise caution.

f. No user shall attempt to make unauthorized uses of resources. That includes, but is not limited to, connecting to a system, or part of a system, to which access is unauthorized. Parts of systems are administratively controlled to protect the integrity of systems and agency operations.

g. No user shall process classified information on a small computer that the DAA has not accredited for that level of classification.

2. **Licensing Agreements**

a. Manufacturers set licensing agreements, and they differ somewhat on the OIG software packages specified in reference (f). All agreements prohibit copying of printed materials, lending the software, or making more than one copy of media.

b. All users are responsible for abiding by the terms of licensing agreements. The ISD has copies of software licensing agreements on large buys. On smaller buys, the agreements accompany distributed software.

c. No software purchased by the OIG may be used on-site or off-site apart from accompanying the OIG owned hardware, unless specifically allowed in the licensing agreement in force at the time the software was purchased. Manufacturers revise licensing agreements at various times even on the same version of the same software. The prohibition generally includes, but is not limited to, the use of the OIG software on privately owned equipment, even if it is being used for work related tasks. The restriction is necessary to conform with the prohibitions in most software

licensing agreements against lending software or making it available to others. Utility programs used to retrieve information in the course of an investigation or audit are exempted from this restriction. However, users of such programs shall ensure that they vigorously avoid infecting systems or violating software-licensing agreements.

3. **Operational Security**

a. Moving or disconnecting small computers may affect network operations or the security of a previously accredited configuration that processes classified material. Therefore, if a small computer is part of a network or accredited configuration, the user shall request support, as specified in reference (g), to move or disconnect the computer.

b. Users shall take all reasonable precautions to secure information resources physically. The precautions apply to on-site use, as well as to transporting or using the resources off-site. For example, resources are in jeopardy if left unattended in plain view in an unlocked hotel room while in travel status or in the passenger compartment of an automobile. All sensitive data stored on the OIG small computers must be protected with adequate ISD approved procedures. The user shall take the same precautions he or she would take to protect valuable personal property, such as a camera.

c. Users shall label all media containing sensitive and classified information in accordance with reference (d).

d. Before using an accredited system, users shall read and understand applicable operational procedures.

4. **Accountability**

a. Beverage and all other liquid containers shall never be placed near computers. If spilled, they may cause extensive damage to the computer or its components.

b. Storage media require special care. Temperature extremes, dampness, fingerprints, scratches, dust, spilled liquids, and pressure may damage the recording media. To protect media from accidental damage, users shall ensure the media are protected according to manufacture's instructions.

c. All provisions of reference (h) shall be followed.

d. Users shall not tamper with or remove drives, memory, circuit boards, or other hardware of small computers issued by the ISD or authorized contractors.

APPENDIX A
REFERENCES

a. IGDINST 7950.3, *Mobile Computing Devices,* May 3, 2007

b. IGDINST 1400.4, *Disciplinary and Adverse Actions,* June 5, 2006

c. IGDINST 4630.3, *Remote Network Access (RNA),* January 16, 2002

d. IGDINST 5200.40, *Security Requirements for Automated Information Systems,* July 20, 2000

e. IGDINST 7950.4, *Computer Antivirus Program,* May 3, 2007

f. IGDINST 7950.2, C*omputer Hardware and Software Management Program,* May 3, 2007

g. IGDINST 8000.2, *Request for Information Systems Directorate (ISD) Services*, March 28, 2002

h. IGDINST 4140, *Property Management Program,* January 3, 2007

APPENDIX B
DEFINITIONS

1. **Accredited configuration** is hardware, firmware, software, procedures, and documentation that have been formally declared by the Designated Approving Authority as approved to operate at a designated security level using a prescribed set of safeguards.

2. **Chief Information Officer (CIO)** is the senior official, appointed by the Inspector General, who is responsible for developing and implementing information resources management in ways that enhance the OIG mission performance through the effective, economic acquisition and use of information. The CIO is the Assistant Inspector General for Administration and Management.

3. **Communications systems** include government owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the Federal Government.

4. **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.

5. **For Official Use Only (FOUO)** is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). FOIA exemptions 2-9 applies to FOUO information. These exemptions cover information containing national security, personal privacy of individuals, trade secrets, proprietary, unauthorized access to, the conduct of OIG operations, and are withheld from release to the public.

6. **Inappropriate Personal Uses.** Users are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. The OIG recognizes that it is necessary occasionally due to the agency mission to engage in activities that would otherwise be considered inappropriate. When the mission requires inappropriate appearances, users shall contact the ISD prior and exercise caution that such uses are necessary. Misuse or inappropriate personal use of government office equipment includes, but is not limited to:

a. Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network. "Push" technology that provides frequent, unsolicited data downloads, and other continuous data streams would also degrade the performance of the entire network and could be considered an inappropriate use.

b. Using the government systems as a staging ground or platform to gain unauthorized access to other systems, unless authorized as mission necessary by appropriate agency authority.

c. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter, unless authorized as mission necessary by appropriate agency authority.

d. Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow users or to the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

e. The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, unless authorized as mission necessary by appropriate agency authority.

f. The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc., unless authorized as mission necessary by appropriate agency authority.

g. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales, or administration of business transactions, sale of goods or services).

h. Engaging in any outside fund raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

i. Use for posting agency information to external newsgroups, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government user, unless appropriate agency approval has been obtained, or uses at odds with the agency's mission or positions.

j. Any use that could generate more than minimal additional expense to the government.

k. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data that includes FOUO, privacy information, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data, unless mission necessary.

7. **Information** is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, maintained in any medium, including but not limited to, computerized databases, paper, microform, or magnetic tape.

8. **Information resources** are any combination of hardware, software, and telecommunications, along with documentation and automated and manual procedures that provide the information necessary to accomplish organizational missions and objectives.

9. **Information system** is the organized collection, processing, transmission, and dissemination of information according to defined procedures, whether automated or manual. It includes people, equipment, and policies.

10. **Malware** is any hardware and/or software that modifies a computer system or records, saves, and/or transmits user information without the knowledge or consent of the user. Malware consists of, but is not limited to, viruses, worms, trojans, adware, spyware, and key loggers.

11. **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.

12. **Small computers** are computers that have self-contained processing units and are easily transportable. The definition includes, but is not limited to, personal computers, programmable calculators and desktop, laptop, palmtop, and notebook computers.

13. **Storage media** includes, but is not limited to, hard disks, floppy disks, zip disks, optical disks, magnetic tapes, and other portable digital media such as Universal Serial Bus (USB) drives, Compact Flash, memory sticks, and USB/Firewire connected external hard drives.

14. **System** is a collection of people, equipment, policies, and methods organized to accomplish an activity.

15. **Virus,** as used in this Instruction, includes all malicious software. Those malicious programs may be viruses, worms, Trojan horses, or bombs.

16. **User** is a person with authorized access to OIG computers, information systems, and/or information technology resources

17. **User non-work time.** Times when the user is not otherwise expected to be addressing official business. Users may, for example, use government office equipment during off duty hours, such as before or after a workday (subject to local office hours), during lunch periods and authorized breaks, or on weekends or holidays (if the user's duty station is normally available at such times).

18. **User support** includes diagnosing and resolving problems about operating and using standard OIG hardware, software, telecommunications, and software applications.