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

May 3, 2007

INSPECTOR GENERAL INSTRUCTION 7950.2

COMPUTER HARDWARE AND SOFTWARE MANAGEMENT PROGRAM

FOREWORD

This Instruction updates the Department of Defense Office of Inspector General, Computer Hardware and Software Management Program. This Instruction defines computer software policies, the chain of responsibility for use and maintenance of computer software, and standard and unauthorized software for the Office of Inspector General

This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Stephen D. Wilson
Assistant Inspector General for
Administration and Management

2 Appendices

A. Purpose. This Instruction updates the Department of Defense Office of Inspector General (DoD OIG), Computer Hardware and Software Management Program.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDINST 7950.2, *Hardware and Software Management Program,* February 9, 2000.

D. Applicability. 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. The standards apply only to computer hardware and software and only to that hardware and software for which there is a wide requirement within the OIG.

E. Definitions. See Appendix B.

F. Policy

1. The OIG shall emphasize standardization and compatibility of computer hardware and software.

2. The Information Systems Directorate (ISD) shall support and manage the OIG standard computer hardware and software.

3. The use of authorized, nonstandard hardware or software is a Component level management decision. The ISD shall not support computer hardware or software that the Director, ISD has not declared an OIG standard. Any OIG Component or user that chooses to use nonstandard computer hardware or software is responsible for the functioning of those information resources. That includes any effect that computer hardware or software may have on the operation of standard computer hardware and software. Even virus free information resources may cause conflicts when introduced into the OIG environment. If the ISD determines that introduced computer hardware or software are causing malfunction of standard computer hardware or software, the ISD will return the user to the standard configuration. The ISD will not assume responsibility for any functionality or data lost by returning to the standard configuration. Any exceptions to this provision must be negotiated between the Component and the ISD.

4. The use of unauthorized hardware and/or software is prohibited on OIG computer systems. Hardware and/or software must be reviewed by ISD, and approved in writing by the Designated Approving Authority (DAA) before it can be connected to, installed on, or used on OIG computer systems. If approved by the DAA, the hardware and/or software becomes authorized, but may remain nonstandard until declared an OIG standard.

5. All previous software standards supported by the ISD as of the publication date of this Instruction will continue to be supported until the Chief Information Officer (CIO) declares the changeover to revised OIG standards is complete.

6. In accordance with reference (a), the ISD, the Office of Security, and the OIG Components shall prepare plans for ensuring that computer hardware and software used in sensitive information systems have appropriate safeguards and controls to prevent loss or harm to the information and to maintain system security, integrity and availability. The OIG Components shall implement and maintain such plans after approval by the DAA, as defined in Appendix B. Computer hardware and software intended for processing Sensitive Compartmentalized Information (SCI) must be security certified and accredited by the DAA.

7. The computer hardware shall be Microsoft compatible and shall meet minimum specifications defined by the ISD.

8. The OIG computer software standards are as follows:

a. *Adobe Acrobat Professional* as the portable document package.

b. *Microsoft* compatible small computer operating system.

c. *Microsoft Access* as the small computer relational data base management package.

d. *Microsoft Excel* as the spreadsheet package.

e. *Microsoft Internet Explorer and Netscape Navigator* as Internet browser packages.

f. *Microsoft Outlook* as the E-Mail and calendar program.

g. *Microsoft Power Point* as the presentation graphics package.

h. *Microsoft Project* as the project management package.

i. *Microsoft Word* as the word processing package.

j. *Symantec Corporate Edition* as the virus scanning package.

k. *Pigeon Communications System* as the agency-wide notification system.

l. *Real Player* as the desktop multi-media file player.

m. Other C2 compliant software required to process classified information.

n. Additional standards (available as justified) are:

(1) *Adobe Photoshop* as the graphics package.

(2) *Macromedia Dreamweaver* and *Adobe Contribute* as the Web authoring package.

(3) *Macromedia Fireworks* as the Web graphics package.

9. The ISD and/or Information System Liaison Working Group shall propose additional changes to the OIG standard software packages according to the procedures outlined in reference (a).

10. Information systems security should be incorporated into all unclassified or classified automated information systems (AIS). Before selecting hardware or software, the following safeguards will be considered:

a. physical security,

b. personnel security,

c. need-to-know,

d. administrative security,

e. information systems security, and;

f. emissions security.

G. Responsibilities

1. The **CIO** shall approve OIG computer hardware and software standards.

2. The **ISD** shall, as soon as the CIO approves a standard:

a. Manage OIG standard computer hardware and software in accordance with references (b) through (g), and other applicable laws, guidelines, regulations, and standards, internal and external. That 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.

b. Review the requirements documentation submitted by the Components, in accordance with reference (d).

c. In coordination with the OIG Components, perform the full range of configuration management. That includes determining what versions, implementation environment, and models of the OIG standards will meet stated functional and technical requirements.

d. Provide user support regarding OIG standard computer hardware and software.

e. Analyze proposed additional or changed OIG computer hardware and software standards, including costs and support plans.

f. Maintain trend analysis data on hardware and software performance as a means to identify root causes of recurring problem areas.

g. Serve as the OIG Network Security Manager (NSM) responsible for the functional security operation of the network. The NSM ensures that the network complies with the requirements for interconnecting to external systems.

h. Provide contracting acquisition support for approved nonstandard hardware and software when the price exceeds the acquisition limit of the Component's Government Purchase Card (GPC).

i. Ensure all OIG computer hardware and software complies with applicable security laws, guidelines, and standards.

j. Develop the AIS security policies, standards, and procedures, to include the use of hardware and software.

k. Perform duties delegated by the DAA regarding any OIG computer hardware or software that process sensitive materials in accordance with reference (b).

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

m. Maintain a list of authorized hardware and software.

3. The **Component Heads** shall:

a. Develop functional requirements documentation for computer hardware and software in accordance with reference (d).

b. Develop procedures for Component level management of computer hardware and software in their mission areas, including monitoring use to ensure that:

(1) All computer hardware and software are used, safeguarded, accounted for, and disposed of in accordance with established policy, laws, licensing agreements, and guidelines, and;

(2) There is adequate capability to support and maintain any nonstandard computer hardware and software within the OIG Component, or;

(3) If requesting ISD support and maintenance for nonstandard computer hardware or software, extraordinary circumstances exist that justify a written negotiated agreement.

c. Communicate their decisions regarding use of nonstandard hardware or software to their users.

4. The **Information Systems Liaison Working Group,** as defined in reference (a), is responsible for monitoring computer hardware and software requirements, and proposing additional or changed OIG standards.

APPENDIX A
REFERENCES

a. IGDINST 8000.1, *Inspector General Automated Information Systems (AIS) Management*, May 3, 2007

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

c. DoD Directive 8000.1, *Management of DoD Information Resources and Information Technology*, February 27, 2002

d. IGDINST 7950.1, *Acquisition of Information Technology Resources,* May 3, 2007

e. IGDINST 7920.5, *Inspector General Small Computer Use,* May 3, 2007

f. IGDINST 4140.1, *Property Management Program*, January 3, 2007

g. Computer Security Act of 1987, Public Law 100-235

APPENDIX B
DEFINITIONS

1. **Accountable Property Officer** is an individual appointed, in writing, by the proper authority, who maintains item and/or financial records in connection with OIG accountable property, irrespective of whether the property is in his/her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use, care, or safekeeping.

2. **Accreditation** is a DAA's assertion of an acceptable level of security risk of an Information System (IS) and its environment. Acceptable security risk is the expectation that an IS will provide adequate protection against unauthorized access, alteration, or use of resources, and against denial of service to authorized users of the IS.

3. **Certification** is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

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

5. **Computer** is a device that has self-contained processing units and are transportable easily. The definition includes, but is not limited to, equipment that may be referred to as palmtop computers, hand held computers, personal digital assistant computers, personal computers, desktop computers, laptop computers, and notebook computers.

6. **Configuration Management** is accounting for, controlling and reporting the planned and actual design of an automated information system throughout its operational life. This includes the computer hardware and software configuration, including the versions, models, and environments to be implemented.

7. **Designated Approving Authority (DAA)** is the official, appointed by the Inspector General who has the authority to accept the security safeguards prescribed for an information system. The DAA issues an accreditation statement that records the decision to accept those standards. The current DAA is the Director, ISD.

8. **Environment** includes elements and mode of operation of an automated information system.

9. **For Official Use Only (FOUO)** is a designation that is applied to unclassified information that may be exempt from the mandatory release to the public under the Freedom of Information Act, (FOIA). The FOIA specifies exemptions 2-9 may qualify information containing national security, personal privacy of individuals, trade secrets, proprietary, unauthorized access to, etc., withheld from release to the public if, by its disclosure, a foreseeable harm would occur.

10. **Functional Requirement** is an expressed computer hardware or software capability needed to accomplish the OIG mission in a more efficient, effective, or economical manner. A functional requirement may fulfill a need for a capability previously unidentified, correct a shortcoming or deficiency in current OIG standards or improve mission effectiveness or efficiency.

11. **Hardware** is the equipment supporting an automated information system.

12. **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.

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

14. **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.

15. **Network Security Manager (NSM)** is the individual responsible for the overall security operation of the network and is the focal point for policy, guidance, and assistance in network security matters. In addition, the NSM ensures that the network complies with the requirements for interconnecting to external systems.

16. **Property Custodian** is an individual appointed in writing by the proper authority to exercise proper custody, care, and safekeeping of the OIG accountable property entrusted to his or her possession or under his or her supervision. He or she may incur pecuniary liability for losses because of failure to exercise his or her obligation.

17. **Software** is a pre-written program used to perform a specific task, such as word processing, desktop publishing, etc.

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

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

20. **User Support** includes diagnosing and resolving problems about operating and using standard OIG computer hardware, software, telecommunications, and software applications.