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

August 3, 2007

INSPECTOR GENERAL INSTRUCTION 4630.2

INTERNET POLICY

FOREWORD

This Instruction provides the policies, procedures, standards and guidelines for the appropriate use of the Department of Defense Office of Inspector General networks and assigns the responsibilities for control and oversight.

The office of primary responsibility for this Instruction is the Information Systems Directorate. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

for Jonilyn M. Poladeck
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) Internet Policy.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDINST 4630.2, *Internet Policy*, August 14, 2002.

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.

E. Definitions. See Appendix B.

F. Policy

1. All employees will read, agree to, and sign the OIG Personal User Network Security Agreement before accessing the classified or unclassified OIG Networks.

2. The OIG employees and contractors shall not create, send, or receive classified information through the Internet or the Non-classified Internet Protocol Router Network (NIPRNET). All classified data transfers shall be performed only on accredited, classified systems. Electronic mail (e-mail) attachments containing sensitive unclassified material will be handled in accordance with reference (a).

3. In accordance with guidance provided by the Chief Information Officer (CIO) Council, government office equipment, including the Internet, shall be used only for official purposes, except as specifically authorized in this Instruction. Employees 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 privilege to use government office equipment for non-government purposes may be revoked or limited at any time. This personal use must not result in loss of employee productivity or interference with official duties. Inappropriate personal use is prohibited. Please see Appendix B, Item 5 for clarification of what constitutes inappropriate personal use. Moreover, such use should 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. Transmission impacts with moderate e-mail message sizes, such as e-mails with attachments smaller than 5 megabytes.

4. This policy in no way prohibits appropriate employee use of government office equipment, including the Internet, for official activities.

5. It is the responsibility of employees 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 must 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. In accordance with references (b) and (c), employees 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 employees wish that their private activities remain private, they should avoid using office equipment such as the computer, Internet, or e-mail. By using government office equipment, employees 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 equipment is made with the understanding that such use is not generally secure, private, or anonymous.

7. Employees shall not send or receive copyrighted graphics or documents through the Internet without the owner's permission.

8. The employee's manager must approve subscriptions to mailing list services. Such subscriptions must be related to an employee's work. Large volumes of e-mail traffic from subscriptions cause delays and other problems for the OIG Networks. Therefore, they should be kept to a minimum.

9. The OIG reserves the right to monitor all Internet communications 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 an employee is not available. Because the OIG is responsible for servicing and protecting its networks, authorized employees may monitor or disclose, or assist in monitoring or disclosing, Internet communications. The Designated Approving Authority (DAA) must provide authorization for this disclosure.

10. Inappropriate personal use of the Internet, to include the inappropriate use of e-mail, streaming audio or video, could result in loss of use or limitations on use of the Internet, suspension of user access to the OIG Networks, disciplinary or adverse action, criminal penalties, and/or the employee being held financially liable for the cost of the improper use.

11. Employees 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.

G. Responsibilities

1. The **OIG CIO** shall:

a. Approve, for the OIG, policies implementing laws and guidelines on Internet use.

b. Provide leadership to manage Internet use within the OIG.

c. Oversee the promulgation of policies and guidance to ensure the most effective and efficient use of Internet resources.

2. The **OIG Component Heads** shall:

a. Establish component-level policies for access and use of the Internet to the extent they deem appropriate to accomplish job responsibilities.

b. Ensure that employees are trained properly in accessing and using the Internet.

c. Ensure employees are informed of OIG policy on appropriate access and use of the Internet.

d. Take appropriate corrective action when employees' use of the Internet violates the provisions of this Instruction.

3. The **Information Systems Directorate (ISD)** shall:

a. Make Internet service available to the OIG employees.

b. Coordinate the administration of all technical aspects of providing Internet services to the OIG through its networks.

c. Have technical control of the OIG Internet connection.

d. Monitor the use of electronic communications to ensure adequate performance and proper use.

e. Use or disclose information obtained during the monitoring process only as required in the performance of official duties.

f. Notify, advise, and assist the CIO of any problem concerning an employee's conduct in accessing and using the Internet and its resources if misuse occurs.

g. Develop Internet security policies, standards, and procedures.

h. Ensure Internet 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 General Services Administration, and the Office of Management and Budget publications.

i. Make decisions on and assist employees with security safeguards for Internet use.

j. Perform the duties delegated by the DAA.

4. **Employee users** of the Internet shall:

a. Read, understand, and abide by this policy and its provisions.

b. Access and use the Internet in accordance with established laws, procedures, and guidelines. Those include, but are not limited to, references (a) through (p).

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

d. Be individually responsible and liable for any disclosures of personal information if the employee chooses to send such information through an electronic communications system provided by the OIG or the Federal Government, or both.

e. Not send classified information through the unclassified OIG network.

f. Refrain from any activities that could congest or disrupt an electronic communications system provided by the OIG or the Federal Government, or both.

g. Properly disconnect from Internet applications when work has been completed. This will free up and ensure appropriate bandwidth for other employees.

h. Keep files and messages stored on-line to a minimum needed to support current projects or job duties. Perform backup of files and e-mail on a regular basis.

i. Refrain from any inappropriate personal uses.

j. Retain ultimate responsibility for keeping the OIG networks malware free in accordance with reference (n).

H. Procedures

1. Employees shall not attempt to disable automatic malware scans. Ultimate responsibility for keeping the network malware free remains with the employee. Employees shall be alert for anything received via the Internet that is unexpected or that may contain malware. Employees should consult with the Technical Support Center in these situations.

2. Employees shall not load any software onto the OIG systems without the written permission of the DAA.

3. When the ISD, detects inappropriate use or abuse of the Internet, the ISD shall provide a detailed hard copy of the employee's accessed sites to the CIO and the Office of Security.

4. If the CIO determines Internet access shall be denied, the CIO shall provide the hard copy logs to the OIG Component Head or his or her designee.

5. If the OIG Component Head requires additional proof, the ISD, shall capture other data and provide the data to the OIG Component Head or his or her designee.

6. The OIG Component Head or his or her designee shall pursue expeditiously any appropriate administrative action or other adverse action with the advice of the Director, HCAS and the Office of Security.

7. If the Office of Security, suspects that the employee has used the Internet to conduct or abet illegal activities, it will notify the appropriate legal authorities.

APPENDIX A
REFERENCES

a. IGDINST 4630.1, *Electronic Mail Policy*, May 22, 2007

b. Electronic Communications Privacy Act of 1986

c. Title 18, U.S.C., Section 2703

d. DoD 5500.7-R, *Joint Ethics Regulation (JER),* August 1993, as changed

e. IGDINST 5400.7, *Freedom of Information Act (FOIA) Program*, May 11, 2006

f. IGDINST 5400.11, *Privacy Act Program*, May 2006

g. IGDINST 5015.2, *Records Management Program*, May 3, 2007

h. IGDINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000, with changes 1 and 2

i. IGDINST 7950.2, *Microcomputer Hardware and Software Management Program*, May 3, 2007

j. DoD Directive 5500.7, *Standards of Conduct*, August 30, 1993, as changed

k. Freedom of Information Act, 5 U.S.C. 552, as amended

l. Privacy Act of 1974, 5 U.S.C. 552a, as amended

m. IGDINST 4630.3, *Remote Network Access (RNA),* May 22, 2007

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

o. IGDINST 7950.4, *Microcomputer Antivirus Program*, May 3, 2007

p. DoD OIG Personal Network Security Agreement

APPENDIX B
DEFINITIONS

1. **Chief Information Officer (CIO).** 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.

2. **Designated Approving Authority (DAA).** 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 DAA is the Director of Information Systems.

3. **Employee.** An OIG employee or contractor who uses computer hardware or software to perform work-related tasks.

4. **Employee Non-Work Time.** Times when the employee is not otherwise expected to be addressing official business. Employees, for example, may use government office equipment during off-duty hours, such as before or after a workday (subject to local office hours), during lunch periods or authorized breaks, or on weekends or holidays (if the employee's duty station is normally available at such times).

5. **Inappropriate Personal Uses.** Employees 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 occasionally necessary due to the agency mission to engage in activities that would otherwise be considered inappropriate. When the mission requires inappropriate appearances, users should exercise caution that such uses are necessary and inform the DAA in advance. 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, such as Pointcast on the RNA, Real Audio, 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 mission necessary.

c. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter, unless mission necessary.

d. Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or 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 mission necessary.

f. The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling (e.g., Fantasy Sports Games), weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc., unless mission necessary.

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, bulletin boards, 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 employee, 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 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.

l. The use of web based email (Yahoo, AOL, etc.), instant chat services (AOL, MSN etc.) or peer to peer (P2P) file sharing software (Napster, Gnutella, Kazaa, etc.).

m. Any action that has the potential to bring discredit upon the Office of Inspector General.

6. **Information Technology.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

7. **Internet.** The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

8. **Malware.** Software designed to infiltrate or damage a computer system, without the owner's informed consent. Malware may consist of a viruses, trojans, worms, rootkits, botnest, spyware, adware or scams.

9. **Minimal Additional Expense**. Employees' personal use of government office equipment is limited to those situations where the government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include, but are not limited to, making a few photocopies, using a computer printer to print a few pages of material, infrequently sending personal E-mail messages, or limited use of the Internet for personal reasons.

10. **NIPRNET.** The Non-classified Internet Protocol Router Network (NIPRNET) provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet.

11. **OIG Environment.** Any computer, media, or network used by the OIG.

12. **Personal Use.** Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan, to seek employment in response to Federal Government downsizing, or communicate with a volunteer charity organization.

13. **Privilege.** In the context of this policy, privilege means that the Executive Branch of the Federal Government is extending the opportunity to its employees to use government property for personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use government office equipment for non-government purposes. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes. Government office equipment, including information technology, includes, but is not limited to, personal computers and related peripheral equipment and software, office supplies, Internet connectivity, and access to Internet services and e-mail.

14. **Sensitive Unclassified Information.** Any information that has not been authorized specifically to be kept classified, but that if lost, misused, disclosed, or destroyed could affect adversely the national interest or the conduct of the OIG operations or Federal programs, or the privacy to which individuals are entitled under the Privacy Act. Typical types of sensitive data are “For Official Use Only,” proprietary, financial, and mission critical information.

15. **Web Site.** A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the “home page” and the linked subordinate information.