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

May 22, 2007

INSPECTOR GENERAL INSTRUCTION 4630.1

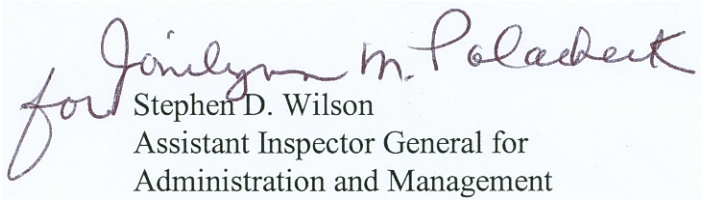
ELECTRONIC MAIL POLICY

FOREWORD

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

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) electronic mail (E-mail) policy.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDINST 4630.1, *Electronic Mail Policy*, August 14, 2002.

D. Applicability and Scope. 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, which is provided support by the OIG when its Office of the Secretary of Defense (OSD) provided equipment interfaces with the OIG network. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

E. Background. The DoD is implementing a Key Management Infrastructure (KMI) to provide engineered solutions for the security of networked computer-based systems. Part of this KMI is a Public Key Infrastructure (PKI) and Public Key Enabling (PKE), consisting of products and services that identify an individual and bind that person to an identified public/private key pair. Programs that carry out or support the mission of the DoD require services such as identification, authentication, confidentiality, technical non-repudiation, and access control.

F. Definitions. See Appendix B.

G. Policy

1. The OIG shall not transfer classified data, as defined in references (a), (b), and (c), via E-mail. Classified data transfers shall be performed only on accredited, classified systems.

2. In accordance with guidance provided by the Chief Information Officer (CIO) Council, Government office equipment, including E-mail, shall only be used for official purposes, except as specifically authorized in this Instruction. End 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 must take place during the end user's 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 must not result in loss of end user productivity or interference with official duties. Inappropriate personal use is prohibited. Please see Appendix B 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, etc.

   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 10 megabytes. Since attachments are a major source of malicious software (malware), attachments of any size on non-official E-mail are discouraged.

3. This policy in no way limits employee use of Government office equipment, including E-mail, for official activities.

4. It is the responsibility of end users to ensure that their personal use of Government office equipment is not falsely interpreted 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.”

5. End users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment or system at any time, including using E-mail. To the extent that end users wish that their private activities remain private, they should avoid using office equipment or systems for personal E-mail. By using Government office equipment or systems, end users imply their consent to disclosing the contents of any files or information maintained or passed through Government office equipment. By using office equipment or systems, consent to monitoring and recording is implied with or without cause, including (but not limited to) using E-mail. Any use of Government E-mail is made with the understanding that such use is generally not secure, private, or anonymous and may be monitored at any time.

6. End users have a primary responsibility to protect OIG systems from malware. They shall be alert to the source of any attachment and shall be alert as to whether they are expecting it. End users shall be alert for anything that is unexpected or may indicate a virus. Users shall consult with the Help Desk in these situations.

7. End users shall not send or receive copyrighted graphics or documents through E-mail without the owner’s permission.

8. End users shall not send or receive illegal or unlicensed software.

9. Use other than described herein is considered to be misuse of information resources.

10. It is a violation of regulations to use Government equipment for personal gain.

11. The OIG E-mail standard is determined by the CIO as specified in reference (d)**.**

12. E-mail messages, like all electronic documents, are considered agency records and are subject to the provisions of references (e), (f), and (g).

13. Many personal E-mail programs now allow "instant messaging" or are Web-enabled, which allows access via any Internet connection. Accessing or logging onto Web-enabled personal E-mail services, or using "instant messaging," via the OIG network impacts on

communication capacity and weakens OIG network defenses. Web-enabled E-mail services and "instant messaging" bypass OIG virus protection. Therefore, end users are not authorized to use OIG resources to access Web-enabled personal E-mail services or "instant messaging" without the express written permission of the DAA.

14. End users may not use personal E-mail services for official business without the express written permission of the DAA.

15. When using Remote Network Access (RNA) to send E-mail from a remote location, users must adhere to the provisions of reference (h)**.**

16. E-mail containing “Sensitive Information” shall be encrypted using a DoD issued certificate.

17. 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.

18. All official E-mail will be digitally signed with a DoD issued certificate.

H. Responsibilities

1. With regard to the OIG E-mail accounts, End Users shall:

a. Check for messages regularly.

b. Dispose of messages (which may include filing, archiving, or deleting) before mailboxes become too full to receive additional correspondence, keeping in mind that E-mail is subject to the provisions of references (e), (f), and (g). The mailbox limit will be adjusted as OIG resources dictates. Users will receive a warning notification prior to reaching the set limit. This includes such boxes as the inbox, sent items, deleted items, etc.

c. Use the E-mail system only for its intended purpose and protect the security of information in accordance with references (b) through (k).

d. Locate Internet addresses of intended message recipients. There is no comprehensive on-line directory of addressees available.

e. Provide their Internet address to those who wish to send them messages.

f. Be alert for unexpected attachments or those that may contain a virus.

g. Dispose of unsolicited messages, such as advertisements, chain letters, jokes, etc., in accordance with the spirit of reference (i). Further distribution of these types of messages is rarely in the spirit of reference (i).

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

i. 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.

j. Not send classified, information through an unprotected electronic communications system unless approved by the DAA. All classified data transfers shall be performed only on accredited, classified systems. Information subject to references (f) and (g) shall be appropriately marked "For Official Use Only" (FOUO) if transmitted electronically.

k. Refrain from any activities that could congest or disrupt an electronic communications system provided by the OIG or the federal government, or both.

l. Refrain from any inappropriate personal uses, including accessing personal E-mail.

m. Store important E-mail messages according to disposition instructions in reference (e).

n. Encrypt E-mail containing "Sensitive" information.

o. Regularly check the OIG Intranet for updated procedures by going to the Information Systems Directorate home page and clicking on the PKI button, or going to https://intra.dodig.mil/AM/ISD/pki/newpki/PKI_index.htm.

p. Immediately report any loss, theft, or misuse of DoD certificates to their supervisor, the Office of Security, and the PKI representative or VO (Verification Official).

q. Inform persons outside of the Federal government with whom they wish to communicate via digitally signed and/or encrypted E-mail of the requirement to obtain a digital certificate from one of DoD's recognized External Certificate Authorities (ECAs).

r. Request for restoring key encryption certificates will be sent by a digitally signed email or in person to the appointed Key Recovery Agent(s) or Key Recovery Officials.

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

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

a. Develop E-mail security policies, standards, and procedures.

b. Ensure E-mail 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.

c. Make decisions on and assist end users with security safeguards for E-mail use.

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

e. Manage the OIG E-mail system.

f. Protect the network from malicious software (malware).

g. Establish and keep current internal lists and other internal addresses, including deleting the mailboxes of end users who have departed the OIG or those who have violated the provisions of this Instruction.

h. Support the OIG E-mail end users.

i. Monitor the use of electronic communications to ensure adequate performance and proper use, as approved by the CIO.

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

k. Notify the end user, the end user's manager, and the ISD of any problem concerning the end user's conduct in accessing and using E-mail.

l. Revoke lost or stolen DoD certificates in accordance with reference (l).

m. Provide and maintain the hardware and software necessary to send encrypted and digitally signed E-mail

n. Recover key encryption certificates in accordance with reference (o).

4. The **Assistant Inspector General for Administration and Management (AIG-A&M)** shall assist and advise when E-mail messages constitute records subject to the provisions of references (e), (f), and (g).

5. The **Inspector General** shall designate the CIO.

6. The CIO shall designate the DAA.

I. Procedures

1. Ultimate responsibility for keeping the OIG systems virus-free remains with the end-user. End users shall be alert for attachments that are unexpected or may indicate a virus. Users shall consult with the Tech Support Desk in these situations.

2. If the end user introduces any software, including that attached to E-mail, into the OIG environment that the ISD did not issue, the user assumes responsibility for the software. This includes any effect that the software may have on the operation of standard hardware and software. Even virus-free software may cause conflicts. If the ISD determines that software introduced by the user is causing a malfunction of standard hardware or software, the ISD shall return the user to the standard configuration. The ISD shall not assume responsibility for any functionality lost by a return to standard configuration. The user is also responsible for operating the software within established laws, guidelines, and procedures, including software licensing agreements.

APPENDIX A
REFERENCES

a. IGDINST O-5200.40, *Security Requirements for Automated Information Systems,* July 20, 2000, as amended

b. DoD Directive 8500.1, *Information Assurance (IA),* October 24, 2002

c. DoD Instruction 8500.2, *Information Assurance (IA) Implementation,* February 6, 2003

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

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

f. DoD Directive 5400.7, *DoD Freedom of Information Act (FOIA) Program,* October 28, 2005

g. DoD 5400.11-R, *Department of Defense Privacy Program,* August 1983

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

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

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

k. DoD Directive 8000.1, *Management of DoD Information Resources and Information Technology*, February 27, 2002, as amended

l. IGDINST 1000.1, *Employee Identification Program*, October 21, 2003

m. DoD Instruction 8520.2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* April 1, 2004

n. DoD X.509 *Certificate Policy for the United States Department of Defense,* Version 9.0, February 9, 2005

o. DoD *Key Recovery Policy for the United States Department of Defense,* August 31, 2003

p. DoD Certificate Policy for External Certification Authorities, April 14, 2004

APPENDIX B
DEFINITIONS

1. **Certificate.** A digital representation of information that, at a minimum, identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.

2. **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 & Management.

3. **Designated Approving Authority (DAA).** The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority. The DAA is the Director, Information Systems Directorate.

4. **Electronic Mail (E-mail).** A means of communication that uses computer-to-computer data transfer technology, normally as textual messages or attached files.

5. **End User.** An OIG employee or contractor who uses computer hardware or software to perform work-related tasks.

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

7. **Hardware Token.** A portable, user controlled, physical device used to generate, store, protect cryptographic information, and to perform cryptographic functions.

8. **Inappropriate Personal Uses.** End 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 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. 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 Remote Network Access, 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 end users 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, 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, engaging in any prohibited partisan political activity, or personal use to sell at-no-cost personal items such as “tickets” or “vacation rentals”.

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 end 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 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.

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

10. **Key Recovery.** The capability for authorized entities to retrieve keying material from a key backup or archive.

11. **Key Recovery Policy.** A named set of rules that specify the conditions under which key recovery information must be created and conditions under which and to whom escrowed keys may be released; it also indicates who are allowable Key Recovery Agent(s) and Key Recovery Officials and how escrowed keys must be maintained.

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

13. **Personal Use.** Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. End users may make limited use under this policy of Government office equipment to seek employment in response to Federal Government downsizing or communicate with a volunteer charity organization.

14. **Privilege.** In the context of this policy, privilege means that the Executive Branch of the Federal Government is extending the opportunity to its end users 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 E-mail software or making configuration changes. Government office equipment, including the E-mail system, 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.

15. **Public Key Enabling (PKE).** The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudation. PKE involves replacing existing or creating new user authentication systems using certificates instead of other technologies, such as userid and password or internet protocol filtering; implementing public key technology to digitally sign, in a legally enforceable manner, transactions and documents; or using public key technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest and/or in transit.

16. **Public Key Infrastructure (PKI).** The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates.

17. **Record.** As defined in 44 U.S.C. 3301, the term includes: all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value or data in them. Is made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of agency business.

18. **Support.** Diagnosing and resolving problems regarding operating and using E-mail.