INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

January 16, 2002

INSPECTOR GENERAL INSTRUCTION 4630.3

SUBJECT: Remote Network Access (RNA)

References: See Appendix A.

A. Purpose. This Instruction updates policy and renames the Office of the Inspector General, Department of Defense (OIG, DoD), Instruction on appropriate use of the Remote Access Server (RAS). It now includes Smartgate and Virtual Private Network (VPN) services to gain remote access to the OIG, DoD, network. The collective access methods are approved to remotely connect to the OIG, DoD, network. Remote Network Access (RNA) includes or is associated with all communication devices/software, firewalls, intrusion detection systems and virus protection applications to ensure security of the OIG, DoD, Network from remote access request to the network.

B. Cancellation. This Instruction cancels IGDINST 4630.3, *Remote Access Server (RAS) Policy*, June 20, 2001.

C. Applicability and Scope. This Instruction applies to the offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; and Director, Intelligence Review. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

D. Definitions. See Appendix B.

E. Policy

1. The OIG, DoD, shall not create, send, or receive classified or sensitive unclassified information through RNA except as approved by the Designated Approving Authority (DAA). This may include encryption when using DoD-approved encryption software.

2. In accordance with guidance provided by the Chief Information Officer Council, Government office equipment, including RNA, 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.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
16 Jan 2002	N/A	-

Title and Subtitle Remote Network Access (RNA)	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 9	

b. General wear and tear on equipment.

c. Data storage on storage devices.

d. Transmission impacts with moderate electronic mail (E-mail) message sizes, such as E-mails with attachments smaller than 10 megabytes.

3. This policy in no way limits end user use of Government office equipment, including RNA, for official activities.

4. In accordance with reference a, users shall not configure privately owned equipment to access RNA, nor shall RAS software, Smartgate, or VPN software be loaded on privately owned equipment. The DoD remote access software may be installed onto Government-furnished computers to enable access to DoD systems and networks.

5. End users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including the RNA. To the extent that end users wish that their private activities remain private, they should avoid using office equipment such as RNA. By using Government office equipment, end 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 OIG Network. Any use of Government resources is made with the understanding that such use is generally not secure, private, or anonymous.

6. End users shall vigorously protect the OIG, DoD, Local Area Network-Wide Area Network (LAN-WAN) from infection with computer viruses or penetration from unauthorized sources while using RNA communications.

7. The OIG, DoD, reserves the right to monitor all RNA communications for the performance of operation, maintenance, auditing, security, or investigative functions. Further, monitoring is used to enforce policies regarding official use and harassment. Because the OIG, DoD, is responsible for servicing and protecting its LAN-WAN, authorized employees may monitor or disclose, or assist in monitoring or disclosing, RNA communications. The Chief Information Officer (CIO) must provide authorization for this monitoring.

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

9. End 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.

F. Responsibilities

1. The **CIO** shall:

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

b. Provide leadership to manage RNA use within the OIG, DoD.

c. Authorize monitoring.

d. Oversee the promulgation of policies and guidance to ensure the most effective and efficient use of RNA resources.

2. **End Users** who use the RNA shall:

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

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

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

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

e. Not send secure, sensitive, classified, or potentially embarrassing information through an electronic communications system provided by the OIG, DoD, the Federal Government, or both (including RNA) unless approved by the DAA.

f. Refrain from any activities that could congest or disrupt electronic communications or allow unauthorized penetration of systems provided by the OIG, DoD, the Federal Government, or both.

g. Properly disconnect from RNA when work is completed. This will free up and ensure appropriate bandwidth for other end users.

h. Install and keep up-to-date antivirus software on any computer used to access the OIG, DoD, LAN-WAN via RNA communications.

i. Refrain from any inappropriate personal use.

j. Not provide login names or passwords to anyone else.

k. Not store or keep persistent login names or passwords via any software (e.g., Gator, Passport, Wallet) accessible to others.

l. Vigorously protect the OIG, DoD, LAN-WAN from virus infection while using RNA communications in accordance with reference d.

m. Physically disconnect from communication modes that provide persistent connection (e.g., a LAN, cable modem, or digital subscriber line) before connecting to RNA.

n. Not configure privately owned equipment to access RNA, nor load RAS software, Smartgate software, or VPN software on privately owned equipment.

o. Not use the same password for different authentication point through remote connection to the OIG, DoD, network.

p. Not use split Internet tunneling for any device using the RNA services.

q. Have a routing switch with built-in firewall and network address translation if they are users of broadband connections (digital subscriber line/cable modems).

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

4. The **Personnel and Security Directorate (PSD), Office of Administration and Information Management (OA&IM),** shall:

a. Perform duties delegated by the DAA.

b. Advise and assist management on appropriate administrative action in accordance with reference e if misuse occurs.

5. The **Information Systems Directorate, (ISD), OA&IM**, shall:

a. Make RNA service available to OIG, DoD, end users based on justified requirements.

b. Coordinate the administration of all technical aspects of providing RNA services to the OIG, DoD.

c. Have technical control of the OIG, DoD, RNA connection.

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

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

f. Notify the end user, the end user's manager, and the PSD, OA&IM, of any problem concerning the end user's conduct in accessing and using RNA.

G. Procedures

1. The end user shall regularly update the antivirus files from the vendor site.

2. The end user shall regularly scan for the presence of viruses.

3. When the ISD, OA&IM, detects inappropriate use or abuse of the RNA, the ISD, OA&IM, personnel shall provide a detailed hard copy of the end user’s accessed sites to the CIO.

4. If the CIO determines RNA shall be denied, the CIO shall provide the hard copy logs to the OIG Component Head or his or her designee and instruct the ISD, OA&IM, to terminate RNA access for the end user.

5. The ISD, OA&IM, shall terminate RNA access.

6. When the OIG Component Head or his or her designee determines that the end user’s RNA access shall be restored, the OIG Component Head or his or her designee shall provide the CIO a justification. The ISD, OA&IM, shall restore RNA access upon CIO approval.

H. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

APPENDIX A
REFERENCES

a. Memorandum for Heads of Defense Components, Under Secretary of Defense (Personnel and Readiness), *Department of Defense* (*DoD) Telework Policy and Guide*, October 22, 2001

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

c. IGDINST 4630.1, *Electronic Mail Policy*, February 1, 2001

d. IGDINST 7950.4, *Microcomputer Antivirus Program*, February 6, 2001

e. IGDR 1400.4, *Disciplinary and Adverse Action*, December 30, 1994

APPENDIX B
DEFINITIONS

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

2. **Designated Approving Authority (DAA).** The official appointed by the Inspector General, DoD, 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, Office of Administration and Information Management.

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

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

5. **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, DoD, 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 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 matte, 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 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 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.

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. **Minimal Additional Expense.** End user's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services and the end user'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 RNA for personal reasons.

8. **Personal Use.** Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. End users are specifically prohibited from using Government office equipment to maintain or support a personal private business. Examples of this prohibition include end users using a Government computer and RNA connection to run a travel business or investment service. The ban on using Government office equipment to support a personal private business also includes end users using Government office equipment to assist relatives, friends, or other persons in such activities. End users 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 other uses cleared through the Ethics Official.

9. **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 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, RNA connectivity, and access to RNA services and E-mail.

10. **Remote Access Server (RAS).** A remote access server is the computer and associated software that is set up to handle users from an outside location seeking access to a network using modems

and other communication lines. Sometimes called a communication server, a remote access server includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to the network.

11. **Remote Network Access (RNA).** The computer and associated software that is set up to handle users from an outside location seeking access to a network using modems and other communication lines.

12. **Sensitive Unclassified Information.** Any information that has not been specifically authorized to be kept classified, but that if lost, misused, disclosed, or destroyed, could adversely affect the national interest or the conduct of OIG, DoD, 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.