U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-05-04

To:	NRC Management Directives Custodians
Subject:	Transmittal of Management Directive 2.6, "Information Technology Infrastructure"
Purpose:	Directive and Handbook 2.6 are being issued to provide information and usage guidance concerning the agency's information technology infrastructure (IT) as it relates to (1) NRC employees and contractors to whom it applies as a condition of a contract or purchase order and (2) Office IT Coordinators. MD 2.6 supports NRC's policy to ensure that a reliable IT infrastructure is made available to agency staff and contractors in accordance with Federal statutes and regulations.
Office and Division of Origin:	Office of Information Services Infrastructure and Computer Operations Division
Contact:	Arnold E. (Moe) Levin, 301-415-7458
Date Approved:	**March 7, 2005**
Volume:	2 Information Technology
Part:	2.6 "Information Technology Infrastructure"
Availability:	Rules and Directives Branch Office of Administration Michael T. Lesar, 301-415-7163 Christy Moore, 301-415-7086

Information Technology Infrastructure

Directive 2.6

Contents

Information Technology Infrastructure
Directive 2.6

Policy
(2.6-01)

It is the policy of the U.S. Nuclear Regulatory Commission to ensure that a reliable information technology (IT) infrastructure is made available to agency staff and contractors in accordance with Federal statutes and regulations. Management Directive (MD) 2.6 will provide information and usage guidance concerning the agency's IT infrastructure as it relates to (1) NRC employees and contractors to whom it applies as a condition of a contract or purchase order and (2) Office IT Coordinators (ITCs). Policy and guidance on telecommunications facilities and services are provided in MD 2.3, "Telecommunications." Policy and guidance on the Automated Information Security Program are provided in MD 12.5, "NRC Automated Information Security Program."

Objectives
(2.6-02)

- To provide basic IT infrastructure and support services for the agency, including interaction with the public, licensees, vendors, and others outside the agency. (021)

- To provide reliable computer and network capabilities in support of the agency's operational, emergency, incident response, and contingency missions. (022)

Objectives
(2.6-02) (continued)

- To ensure adherence to the agency's IT architecture and other applicable standards. (023)

- To ensure adherence to Federal statutes and regulations affecting the agency's IT infrastructure. (024)

- To provide guidance to agency staff and contractors on using the IT infrastructure responsibly. (025)

Organizational Responsibilities and Delegations of Authority
(2.6-03)

Executive Director for Operations (EDO)
(031)

- Acting as the Agency Head for IT, establishes a capital planning and management oversight process for IT infrastructure investments. (a)

- Ensures that NRC's planning and budgeting for IT infrastructure is consistent and is integrated with the NRC's overall planning, budgeting, and performance management process. (b)

- Ensures that program and IT officials participate in the planning and budgeting process for IT infrastructure. (c)

- Operates in concert with the Deputy Executive Director for Information Services and Administration and Chief Information Officer (DEDIA) and the IT Senior Advisory Council to provide an Executive/Investment Review Committee as required by the Office of Management and Budget (OMB). (d)

- Ensures that statutory responsibilities regarding IT infrastructure investments and their oversight are appropriately assigned to the DEDIA. (e)

Organizational Responsibilities and Delegations of Authority
(2.6-03) (continued)

Deputy Executive Director for Information Services and Administration and Chief Information Officer (DEDIA)
(032)

- Provides NRC with a reliable and effectively managed basic IT infrastructure that supports the agency's computing and information management (IM) needs. (a)

- Establishes and maintains agencywide policies, architectures, and standards governing the IT infrastructure. (b)

- Authorizes, directly or by designee, exceptions to or deviations from this directive within the limitations of authority set by Federal statutes and regulations. (c)

- Ensures agency compliance with Executive Order 13103 on computer software piracy. (d)

Inspector General (IG)
(033)

Conducts investigations and/or audits related to all NRC programs and operations, including the agency's IT infrastructure.

Director, Office of Information Services (OIS)
(034)

- Plans for the funding and development of the agency's basic IT infrastructure. (a)

- Works with offices to plan and acquire all IT hardware, software, and services that are not included in the basic IT infrastructure. (b)

Organizational Responsibilities and Delegations of Authority
(2.6-03) (continued)

Director, Office of Information Services (OIS)
(034) (continued)

- Supports the IT infrastructure during its entire life cycle. (c)
- Ensures that the agency's IT infrastructure is in compliance with applicable policies, architectures, and standards. (d)

Director, Office of Nuclear Security and Incident Response (NSIR)
(035)

- Directs and operates the agency's classified IT program. (a)
- With the cooperation of OIS, plans, implements, and provides IT infrastructure support for infrastructure resources in the NRC Operations Center. (b)

Office Directors and Regional Administrators
(036)

- Determine office-specific functional requirements for IT infrastructure resources and services. (a)
- Annually prepare and submit to OIS office-specific functional requirements for IT infrastructure resources and services in support of agencywide IT planning. (b)
- Ensure that the staff adheres to the agency's IT infrastructure architecture and standards in accordance with the agency Enterprise Architecture. (c)

Organizational Responsibilities and Delegations of Authority
(2.6-03) (continued)

Office Directors and Regional Administrators
(036) (continued)

- Participate in agencywide planning of IT infrastructure resources in accordance with MD 2.2, “Capital Planning and Investment Control.” (d)

- Work with OIS to plan, fund, and acquire office-managed IT in accordance with MD 2.2. (e)

- Work with OIS in its efforts to provide and ensure effective implementation of IT infrastructure support for infrastructure resources. (f)

- Appoint an ITC for the office and work with OIS to ensure that the ITC has adequate time and training to perform his or her duties. (g)

- Ensure that ITCs adhere to the instructions provided by OIS. (h)

- Notify OIS of ITC appointments. As ITC appointments are made or changed, contact the Chief of the Network Operations and Customer Services Branch, OIS, or designated staff. (i)

- Ensure that the staff is properly trained to make effective use of IT in performing its functions. (j)

- Ensure that the staff uses IT in accordance with the guidance in Handbook 2.6 and other NRC management directives, Executive Orders, pertinent laws, regulations, circulars, directives of other Federal agencies, and published NRC guidance (e.g., NRC Yellow Announcements) and takes action to correct inappropriate use of IT resources. (k)

Organizational Responsibilities and Delegations of Authority
(2.6-03) (continued)

Regional Administrators
(037)

Assume the responsibilities of office directors and, with the concurrence of OIS, provide IT infrastructure support for resources in their respective regions and resident sites.

Director, Infrastructure and Computer Operations Division (ICOD), Office of Information Services (OIS)
(038)

Directs the development and operation of the agency's IT infrastructure and manages the services provided.

Director, Division of Contracts (DC), Office of Administration (ADM)
(039)

Directs and coordinates the agency's contracting and purchasing activities, including those involving IT resources.

Director, Division of Administrative Services (DAS), ADM
(0310)

- With the support of OIS, oversees property management of NRC equipment, including IT hardware, through tagging and inventory programs. (a)

- Ensures and coordinates agency compliance with property certification requirements in accordance with MD 13.1, "Property Management." (b)

Organizational Responsibilities and Delegations of Authority
(2.6-03) (continued)

Senior Information Technology Security Officer, Program Management, Policy Development, and Analysis Staff (PMAS), OIS
(0311)

- Ensures agency compliance with information security legislation and guidance. (a)
- Provides oversight and guidance for the information systems security incident response procedures and processes. (b)
- Serves as the primary IT security point of contact between the various security officials throughout NRC, and also with NRC management, including OIS and the Office of the Executive Director for Operations (OEDO). (c)
- Coordinates the activities of the OIS Computer Security Staff in responding to, handling, and reporting information systems security incidents involving any computers that are processing sensitive information, Safeguards Information (SGI), or classified information. (d)
- Reviews and approves security plans for processing sensitive information, Safeguards Information (SGI), and classified information. (e)

Applicability
(2.6-04)

- The policy and guidance in this directive and handbook apply to all NRC staff and all NRC contractors to whom they apply as a condition of a contract or a purchase order. (041)

Applicability
(2.6-04) (continued)

- Unless otherwise specified, this directive and handbook cover policy and guidance for acquiring and using the NRC's IT infrastructure resources, including the basic agencywide IT infrastructure provided and maintained by OIS, as well as the IT infrastructure provided and maintained by other offices. (042)

Handbook
(2.6-05)

Handbook 2.6 describes the processes and procedures for acquiring and using the NRC's IT infrastructure (hardware, software, and support services).

References
(2.6-06)

Executive Order 13103, "Computer Software Piracy."

U.S. Nuclear Regulatory Commission Management Directives—

2.2, "Capital Planning and Investment Control."

2.3, "Telecommunications."

2.4, "Acquisition of Information Technology Resources."

2.7, "Personal Use of Information Technology."

3.2, "Privacy Act."

3.14, "U.S. Nuclear Regulatory Commission External Web Site."

11.1, "NRC Acquisition of Supplies and Services."

12.2, "NRC Classified Information Security Program."

References
(2.6-06) (continued)

12.5, “NRC Automated Information Security Program.”

12.6, “NRC Sensitive Unclassified Information Security Program.”

13.1, “Property Management.”

United States Code

Federal Information Security Information Act of 2002 (FISMA) (Pub. L. 107-347, 116 Stat. 2899).

Government Information Security Reform Act of 2000 (GISRA).

Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

Information Technology Infrastructure

Handbook

2.6

Contents

Part I
Information Technology Infrastructure

General (A)

Unless otherwise specified in this document, Management Directive (MD) 2.6 covers policy and guidance for obtaining and using the basic agencywide information technology (IT) infrastructure provided and maintained by the NRC's Office of Information Services (OIS). Specifically, that infrastructure includes standard desktop workstations with a standard suite of productivity software, network connectivity and file/print services, Web and application hosting, Internet connectivity, and remote access services (information on the standard infrastructure can be found on the Network Operations and Customer Services Branch [NOCSB] Web site). In addition, MD 2.6 covers policy and guidance for acquiring and using the related IT infrastructure support services provided by OIS. Specifically, those services include installation and removal, upgrades, moves, helpdesk support, hardware/software maintenance, network access, and operations services, as well as the office-owned IT infrastructure (e.g., laptops, personal printers, etc.) provided and maintained by other offices and regions.

Infrastructure Planning (B)

Each year, the OIS Infrastructure and Computer Operations Division (ICOD) provides a draft of the Information Technology and Information Management (IT/IM) Budget Planning and Guidance to the NRC offices and regions for the future fiscal year. Meetings are then held to answer questions, acquire an understanding of office and regional IT/IM plans for the planning period, and accept updates to the plan. (1)

During these meetings between OIS and office and regional representatives, OIS also shares its long-range IT infrastructure plans with the offices and regions. Consequently, in preparation for these meetings, offices and regions should document their

Infrastructure Planning (B) (continued)

short- and long-term IT initiatives and any possible infrastructure changes needed to support those initiatives. OIS will work with the offices and regions to address their needs for either the current or future planning period. (2)

Guidelines for Use (C)

NRC provides an agencywide IT infrastructure for official, authorized, and limited personal use by NRC employees. (See MD 2.7, "Personal Use of Information Technology," for information on limited personal use.) NRC also provides IT infrastructure for official use by certain NRC contractors as a condition of a contract or a purchase order. (1)

The following guidelines apply to all users of the NRC's IT infrastructure resources: (2)

- Use of the NRC's IT infrastructure constitutes consent to monitoring. A consent to monitoring warning banner is displayed on workstations at initial user sign on. (See the IT Security section of the NOCSB Web site for the full text of this warning banner.) (a)

- Agency electronic mail is for official and other authorized purposes. Classified information may not be transmitted via agency electronic mail. Safeguards Information (SGI) may be transmitted provided it has first been properly encrypted using encryption algorithms approved by the National Institute of Standards and Technology or the National Security Agency. Contact the OIS Computer Security Staff for assistance in identifying approved methods of encryption. (See MD 12.5, "NRC Automated Information Security Program," and MD 12.6, "NRC Sensitive Unclassified Information Security Program," for guidance pertaining to the secure use of the NRC's IT infrastructure.) Electronic mail messages may constitute official agency records and should, therefore, be handled accordingly. (See MD 3.53, "NRC Records Management Program," for additional information.) (b)

Guidelines for Use (C) (continued)

- Internet resources shall be used only to access, download, and print information for official business and other authorized purposes; users should observe applicable copyright restrictions when downloading material. Access to prohibited categories of Internet sites (such as criminal skills, gambling, hate speech, and pornography/sex) has been blocked; however, each individual is responsible for using the resources in accordance with applicable regulations. (c)

- Software shall be used in accordance with applicable licensing agreements. (d)

Prohibited Use (D)

The following examples constitute prohibited uses of the NRC's IT infrastructure resources: (1)

- Use for activities that are illegal, inappropriate, or construed as justifiably offensive to fellow employees or the public. (a)

- Use as a staging ground or platform to gain unauthorized access to other systems. (b)

- Use to create, download, view, store, copy, transmit, or receive sexually explicit or sexually oriented materials or materials related to illegal gambling, illegal weapons, or terrorist activities. (c)

- Use for commercial purposes or in support of "for-profit" activities or other outside employment or business activity, and any other illegal activities or activities that are otherwise prohibited. (d)

- Use to acquire, download, install, reproduce, distribute, transmit, or use software in violation of copyright laws or licensing agreements (see Executive Order 13103 on computer software piracy). See the NOCSB Web site listed in Appendix A for acceptable proof of compliance with this order. (e)

Prohibited Use (D) (continued)

- Movement of any IT infrastructure by any employee or contractor without the appropriate approval(s) from OIS or a designee. (f)

- Connecting or disconnecting any IT equipment (e.g. laptops, personal digital assistants (PDAs), modems, etc.) to or from IT infrastructure by any employee or contractor without the appropriate approval(s) from OIS or a designee. (g)

Part II
User Procedures

General (A)

OIS and the regional support staff provide agencywide basic IT infrastructure (including standard desktop workstations with a standard suite of productivity software, file/print services, Web and application hosting, Internet connectivity, and remote access services) to NRC staff and to select NRC contractors when required as a condition of a contract or a purchase order. Offices provide office-owned IT infrastructure, such as laptop computers, personal printers, personal digital assistants (PDAs), and other equipment and software, as necessary, to meet specific business needs. Only OIS, regional support staff, or a designee provides installation/removal, upgrades, moves, helpdesk support, maintenance, network access, and operations services to support the IT infrastructure at NRC Headquarters and, as appropriate, at regional offices and the NRC's Technical Training Center (TTC). Regional IT offices provide additional infrastructure for the regions and resident sites.

Support (B)

Users at NRC Headquarters (NRCHQ) should contact the OIS Customer Support Center (CSC) for support related to IT infrastructure resources (see Appendix A for contact information). The Network Operations and Customer Services Branch (NOCSB) Web site can also provide users with support information. Link information for the NOCSB Web site can be found in Appendix A. Service levels for completion of requests at NRCHQ are also posted at the NOCSB Web site. (1)

Users at the regional offices, resident sites, and the TTC must contact their regional office IT support staff for support related to IT infrastructure resources. (See Appendix A for contact information.) Users at NRCHQ must contact the CSC to request maintenance of desktop workstations and peripherals. (2)

Support (B) (continued)

- The CSC staff will request information such as user name and local area network (LAN) identifier (ID), location, personal computer (PC) tag number, and description of the problem. (a)

- The CSC staff will suggest steps the user can take to attempt to resolve or more closely determine the cause of the problem. (b)

- If the problem cannot be resolved by telephone, the CSC will dispatch a staff member to the user's NRC work location. (c)

In addition, NRCHQ users must contact the CSC to request assistance with software installed on desktop workstations. (3)

- The CSC staff will request information such as user name and LAN ID, location, PC tag number, and description of the problem. (a)

- The CSC staff will attempt to guide the user through the steps necessary to accomplish the required task. (b)

- The CSC does not provide training in the use of applications; training is available through the Professional Development Center (PDC) (see Appendix A). (c)

Moves, Additions, and Changes (C)

Requests for installations, moves, upgrades, or removals of desktop workstations, software, or peripherals are approved and conveyed by the Office IT Coordinators (ITCs) to the CSC at NRCHQ and by the regional office IT support staff in the regional offices. NRCHQ users can identify their ITC by viewing the NOCSB Web site (see Appendix A).

- All requests for installations, moves, upgrades, or removals of desktop workstations, software, or peripherals in regional offices must be approved by the regional office IT support staff. (1)

Moves, Additions, and Changes (C)
(continued)

- Requests at NRCHQ for network access (direct and remote) and access to server-based applications are approved and conveyed by the ITC to the CSC or the application owner. If remote access is granted by the CSC, users must sign the NRC's Remote Access Agreement. See the NOCSB Web site for the full text of the agreement. (2)

- NRCHQ requests for installation of personally owned hardware and software are considered on a case-by-case basis. OIS does not provide maintenance services for personally owned items. (3)

- NRC-provided hardware and software may be made available for use at an offsite location, including an employee's home. OIS does not provide support services at employees' homes or other offsite locations (except certain pre-approved contractor sites), other than the assistance provided by the CSC via telephone. (4)

Part III
IT Coordinator Procedures

IT Coordinator's Role (A)

The IT Coordinator (ITC) serves as the office representative for IT infrastructure resources at NRC Headquarters (NRCHQ). The regional IT support staff, in addition to the roles and responsibilities described in Part IV of this management directive, performs the role of the ITC in the regions. The ITC acts as liaison between office staff and OIS to ensure that IT infrastructure service requests are completed. The offices must notify the Chief of the Network Operations and Customer Services Branch (NOCSB) or designee of any changes in ITC appointments. The ITCs fulfill the following functions: (1)

- Serve as the office point-of-contact for IT infrastructure service requests involving microcomputer hardware, software, and networks, as well as telephones, pagers, and other telecommunications equipment. (a)

- Serve as the point-of-contact for coordinating all microcomputer equipment moves and network account moves, including submitting move requests to the Customer Support Center (CSC). (b)

- Attend OIS briefings on IT issues. (c)

- Serve as office liaisons between office staff and OIS to coordinate agencywide infrastructure software upgrades. (d)

- Advise OIS of any changes to the office computing environment. (e)

- Interact with the CSC to provide notification of office-specific issues. (f)

IT Coordinator's Role (A) (continued)

- Relay information from OIS in a timely manner to the appropriate staff within the ITC's respective office. (g)

The following sections provide guidance to assist the ITCs in fulfilling these functions. (2)

Acquisition (B)

"Acquisition" is used in this section to mean the acquisition of IT resources by all means, not only purchases. (1)

Requests for the purchase of IT infrastructure that is not included in the agency's basic IT infrastructure must be submitted to the Infrastructure and Computer Operations Division (ICOD), OIS, by the Office ITC for approval before purchase. (2)

For acquisitions that involve multiple copies of software, Office ITCs should investigate the possibility of using software that employs an open license agreement. Such agreements may provide a cheaper and more manageable solution to buying multiple copies of software. Inasmuch as open license agreements vary for each vendor, read the agreements thoroughly before making any purchases. (3)

Planned acquisition or development of IT resources (such as new application systems, major modifications of existing application systems, and changes to the production operating environment (POE)) is subject to the agency's Capital Planning and Investment Control (CPIC) process and the Software Development Life Cycle Management Methodology (SDLCMM). The CPIC process can be found in MD 2.2, "Capital Planning Investment and Control." Policies and procedures for the SDLCMM can be found in MD 2.5, "System Development Life Cycle Management Methodology (SDLCMM)." (4)

All planned acquisitions or projects that involve changes to the NRC's POE are also subject to the Infrastructure Development Process Model (IDPM) and must be coordinated

Acquisition (B) (continued)

with the Development and Deployment Branch (DDB), ICOD, OIS, by contacting the Chief of DDB. Policies and procedures for the IDPM can be found at the NOCSB Web site (see Appendix A). (5)

All planned acquisitions or projects that involve changes to the NRC's POE must be approved by ICOD and must meet the following procedural requirements: (6)

- Approval by the NRC Infrastructure Information System Security Officer (ISSO). At NRCHQ, this process is initiated by submitting a request on the Consolidated Test Facility (CTF) Web page on the NOCSB Web site (see Appendix A). (a)

- Approval by the ICOD Operations Change Control Board for production operations. At NRCHQ, this process is initiated by submitting a Technical Change Request (TCR) on the CSC Network Operations Web page on the NOCSB Web site (see Appendix A). (b)

If planned acquisitions or projects require OIS Web and application hosting services, those services must be requested by contacting the Chief of the Computer Operations and Telecommunications Branch (COTB), (ICOD/OIS), and filling out the Service Level Agreement and hand-off documents. These documents can be found at the Computer Operations Hosting page of the Computer Operations Web site (see Appendix A). (7)

Purchases to be made with agency purchase cards require approval by the responsible office directors or their designee (usually the Office ITC) and ICOD/OIS. (8)

- Purchase card acquisitions from the Infrastructure Services and Support Contract (ISSC) Catalog do not require further ICOD/OIS authorization; other purchases require ICOD/OIS authorization, which may be requested by sending an e-mail message to IDIB@nrc.gov. (a)

Acquisition (B) (continued)

- Purchase card acquisitions are subject to the agency rules detailed in the NRC Purchase Card Program Procedures Handbook; see the Purchase Card Information link on the Office of Administration's Division of Contracts Web site (in Appendix A). (b)

Support (C)

At NRCHQ, the CSC serves as the primary point-of-contact for requesting support services from OIS for IT infrastructure resources for all ITCs. See Appendix A for CSC Helpdesk contact information. (1)

OIS customer support staff are also available to answer questions and provide assistance for ITCs. Contact information is available on the NOCSB Web site (see Appendix A). (2)

Service levels for completion of requests are posted at the NOCSB Web site (see Appendix A). (3)

Network Access (D)

Access to the NRC's local area and wide-area networks (LAN/WAN) is provided only to those who meet the security requirements and need access for the performance of their duties. A user identifier (user ID) and associated passwords are required to access the LAN/WAN. User IDs are issued to specific individuals. Sharing of user IDs and passwords is not permitted. (1)

Requests for NRC network access (direct and remote) and access to server-based applications at NRCHQ are conveyed by the ITC to the CSC or the application owner. If remote access is granted by the CSC, users must sign the NRC Remote Access Agreement. See the NOCSB Web site (in Appendix A) for the full text of the agreement. (2)

Network Access (D) (continued)

- NRC employees must have a "Q" or an "L" security clearance or a Section 145b waiver before submitting a network access request. (See MD 12.5, "NRC Automated Information Security Program.") (a)

- Contractors must have a "Q" or an "L" security clearance or an IT Level I or II access authorization before submitting a network access request. (b)

Contractor access authorization (IT Level I or II) can be determined by looking at the upper right-hand corner of the contractor's badge or by contacting the contractor's Project Officer. (3)

Desktop Workstations (E)

OIS provides a standard desktop workstation for each employee and select contractors, as necessary. Requests for new workstations at NRCHQ should be conveyed by the responsible ITC to the CSC. Unless otherwise specified in the request, each workstation will be configured for network and Internet access and will have the standard suite of productivity software (word processing, presentation, and spreadsheet applications, as well as electronic mail and calendaring). Additional information on the standard infrastructure can be found on the CSC Web site (see Appendix A). (1)

Requests for installation and upgrades of desktop workstations, software, and peripherals at NRCHQ should be approved and conveyed by the ITC to the CSC. Requests for removal of software that is no longer needed by a user should also be conveyed by the ITC to the CSC. (2)

- Some items at NRCHQ require testing in the Computer Testing Facility (CTF) before installation on the IT infrastructure. This requirement generally applies to previously untested hardware or software that is to be installed on the network, or items that are to be used by multiple users or that may otherwise affect

Desktop Workstations (E) (continued)

the NRC's IT infrastructure. The CSC will notify the ITCs if such testing is required. CTF testing can be initiated by submitting a request on the CTF Web page on the NOCSB Web site (see Appendix A). (a)

- Use of shareware/freeware/evaluation copies of software is permitted in accordance with applicable copyright laws if the Office ITC determines that use of the software is required to meet an agency business need. (b)

- Requests for installation of personally owned hardware and software (e.g., laptops, personal digital assistants (PDAs)) are considered on a case-by-case basis; authorization requires each user to sign an agreement indicating that he or she understands that NRC is not responsible for loss or damage to personal items or data and certifying that the software will be used in accordance with applicable copyright laws. The agreement is provided to the user before the software is installed. OIS or regional IT support staff do not provide maintenance services for personally owned items. (c)

NRC-provided hardware and software may be made available for use at an offsite location, including an employee's home. OIS or regional IT support staff do not provide support services at employees' homes or other offsite locations (except certain pre-approved contractor sites), other than the assistance provided by the CSC or regional IT support via telephone. At NRCHQ, Office ITCs shall notify the Chief of NOCSB, ICOD/OIS, of proposed moves of hardware or software to offsite locations, except in cases of sensitive items for which an employee has signed an NRC Form 119. (3)

- NRC employees may use laptop computers and PDAs at offsite locations without notifying OIS; however, the NRC employee shall have signed an NRC Form 119 accepting responsibility for the sensitive item. (a)

Desktop Workstations (E) (continued)

- Authorization for home use of desktop workstations, peripherals, or software requires users to sign an agreement indicating that they understand that NRC is not responsible for loss or damage to personal items or data, and certifying that the software will be used in accordance with applicable copyright laws. The agreement will be provided when installations are authorized. (b)

- Office ITCs and contract Project Officers must notify their Property Custodians when NRC-owned equipment is relocated to or from offsite locations. (OIS notifies Property Custodians when equipment is relocated within NRC Headquarters.) The Office of Administration (ADM) maintains a list of Property Custodians on its Division of Administrative Services Web site (see Appendix A). (c)

Maintenance and Support (F)

At NRCHQ, the ITC may have users request maintenance of desktop workstations and peripherals by contacting the CSC directly. The CSC will request information, such as user name and LAN ID, location, PC tag number, and description of the problem. (1)

- The CSC helpdesk staff will suggest steps the user can take to attempt to resolve or more closely determine the cause of the problem. (a)

- If the problem cannot be resolved by telephone, the CSC will dispatch a staff member to the location. (b)

At NRCHQ, the ITC may have users also contact the CSC directly to request assistance with software installed on desktop workstations. Again, the CSC will request information, such as user name and LAN ID, location, PC tag number, and description of the problem. (2)

Maintenance and Support (F) (continued)

- The CSC helpdesk staff will attempt to guide the user through the steps necessary to accomplish the required task. (a)

- The CSC does not provide training in the use of applications; training is available through the Professional Development Center (PDC). See the PDC's Web site (Appendix A) for more information. (b)

Equipment Relocation and Removal Requests (G)

OIS pays a monthly fee for each issued standard desktop workstation, including those that are not currently in use. For that reason, as well as security reasons, all unused desktop workstations must be turned in to OIS unless an incoming employee is expected to need the workstation within 2 weeks following the departure of the previous user. (1)

Requests at NRCHQ for relocating desktop workstations and attached peripherals are made by submitting the move form, which can be downloaded from the NOCSB Web site (see Appendix A). Requests in the regions should be made to the regional IT support staff. (2)

- Users moving from one office to another within the same geographic area (such as NRC HQ) are expected to have their desktop workstations move with them. The office from which the user is moving may elect to retain special hardware or software. In such cases, the responsible ITC will note the hardware and/or removal requirements when requesting relocation of the equipment. The ITC can verify removal of special hardware or software by confirming the removal request is complete via the agency's IT request tracking system (currently Magic). When users are moving from one office to another within the same geographic area (such as NRCHQ), ITCs from each office should coordinate with each

Equipment Relocation and Removal Requests (G) (continued)

other to prevent duplicate, conflicting, and incomplete requests. (a)

- Requests for removal of excess desktop workstations and related hardware at NRCHQ are made by the ITC to the CSC or (especially for high-performance workstation equipment) through an ADM Labor Services request. Labor Services requests (submitted through the online ADM system or using NRC Form 30, “Request for Administrative Services”) should specify that the equipment is to be moved to O-2 A1. (The NRC staff in O-2 A1 will sort, redistribute, or arrange for disposal of the items. Hard drives will be wiped with an overwrite process or will be removed and destroyed.) (b)

Part IV
Regional IT Support Staff

Regional IT Support Staff Role

The role of the regional staff and management, in essence, integrates planning, funding, development, deployment, support, and maintenance activities for local systems (regions and resident sites) under the agency's life cycle management process for information technology (IT). To some extent, the regional IT support role encompasses all of the infrastructure support functions of OIS on a smaller scale. As a result, the regional IT function and process encompass responsibility and authority similar to the way OIS encompasses them, within the constraints of agency policy. OIS works closely with the regions to manage IT deployment in the agency overall.

Glossary

Basic information technology (IT) infrastructure. Agencywide information technology (IT) infrastructure provided by OIS, including standard desktop workstations with a standard suite of productivity software, file and print services, Web and application hosting, Internet connectivity, and remote access services.

Classified information. Information designated as "National Security Information," "Restricted Data," or "Formerly Restricted Data" (Management Directive 12.2, "NRC Classified Information Security Program").

IT infrastructure. IT investments that support common user systems, communications, and computing infrastructure, including equipment and software systems and the facilities and services that interconnect and support them. These investments usually involve multiple mission areas and might include general local area network/wide-area network (LAN/WAN), desktops, and data centers. Use of this term includes both basic and office-owned IT infrastructure.

IT infrastructure support. Installation or removal, upgrades, moves, helpdesk support, maintenance, network access, and operations services.

Local IT Infrastructure. See "Office-owned IT infrastructure."

Office-owned IT infrastructure. Non-basic IT infrastructure that is purchased by the program or regional offices. This infrastructure also includes IT infrastructure that is specific to a location.

Open License Agreement. An agreement with a software provider that allows a client to purchase a single copy of the software and to purchase additional licenses so that a single copy of software can be installed for multiple users.

Glossary (continued)

Personally owned hardware and software. Hardware and software that has not been provided by NRC.

Safeguards Information (SGI). Sensitive but unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities (as noted in 10 CFR Part 73).

Appendix A
Contacts

Regional Information Technology (IT) Infrastructure Contact Information

Region I
- Telephone: 610-337-5050

Region II
- Telephone: 404-562-4444
- Electronic mail: R2_HELP

Region III
- Telephone: 630-829-9541
- Electronic mail: HELP3

Region IV
- Telephone: 817-860-8268
- Electronic mail: R4HELP

NRC Headquarters Contact Information

IT Customer Support Center (CSC)
- Telephone: 301-415-1234
- Electronic mail: CSC
- Personal visit: T-4 C18

OIS Computer Security Staff: 301-415-7430

Web Pages

NOCSB Web site: http://csb.nrc.gov

Professional Development Center (PDC): http://papaya.nrc.gov/ie/index.html

Computer Operations Web site http://www.internal.nrc.gov/OCIO/ICOD/COTB/Operations/index.html

Appendix A (continued)

Office of Administration's Division of Contracts http://www.internal.nrc.gov/ADM/DCPM/DCPM_HOME_PAGE.html

Office of Administration's Division of Administrative Services Web site: http://www.internal.nrc.gov/ADM/DAS/listpage.html