OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

Audit of NRC's Telecommunications Program

OIG-05-A-13 June 7, 2005

AUDIT REPORT

All publicly available OIG reports (including this report) are accessible through NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

June 7, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum**/RA/**
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S TELECOMMUNICATIONS PROGRAM (OIG-05-A-13)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Telecommunications Program*.

This audit found that improvements are needed to strengthen controls over the use of the Nuclear Regulatory Commission's (NRC) telecommunications services and the physical security of NRC telecommunications systems. Specifically, NRC's telecommunications program oversight does not ensure that:

- Employees and contractors are using NRC's telephone system appropriately and that phone bills are accurate.
- Employees are consistently using the Government calling card for long-distance calls while on official travel.
- The agency's secure cell phone users are receiving the best possible coverage to meet their needs.
- Physical security requirements are enforced pertaining to telephone equipment closets.

During an exit conference held May 18, 2005, the agency generally agreed with the findings and recommendations in this audit report and provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

If you have any questions, please call Beth Serepca at 415-5911 or me at 415-5915.

Attachment: As stated

Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
William N. Outlaw, Acting Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Frank J. Congel, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Acting Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

EXECUTIVE SUMMARY

BACKGROUND

The Nuclear Regulatory Commission's (NRC) telecommunications program includes local and long-distance voice services, voicemail, videoconferencing, and personnel communications equipment (e.g., calling cards, cell phones). The Office of Information Services (OIS) provides overall guidance and direction for the agency's non-secure telecommunications systems and equipment. The Office of Nuclear Security and Incident Response manages NRC's secure telecommunications systems and equipment. This audit focused primarily on the agency's non-secure telecommunications systems, although auditors also reviewed the agency's use of secure cell phones.

PURPOSE

The audit objectives were to evaluate (1) controls over the use of NRC telecommunications services and (2) the physical security of NRC telecommunications systems.

RESULTS IN BRIEF

Improvements are needed to strengthen controls over the use of NRC's telecommunications services and the physical security of NRC telecommunications systems. NRC's telecommunications program oversight does not ensure that:

- Employees and contractors are using NRC's telephone system appropriately and that phone bills are accurate.
- Employees are consistently using the Government calling card for long-distance calls while on official travel.
- The agency's secure cell phone users are receiving the best possible coverage to meet their needs.
- Physical security requirements are enforced pertaining to telephone equipment closets.

Appropriate Usage Is Not Ensured

NRC's telecommunications program oversight does not ensure that employees and contractors are using NRC's telephone system appropriately and that phone bills are accurate. Specifically,

- OIS performs subjective and limited billing reviews that do not fulfill the requirements in MD and Handbook 2.3.

- OIS does not conduct sufficient inventories to ensure that all phone lines and circuits for which NRC pays each month are used and necessary.
- OIS does not restrict use of the headquarters toll-free number in accordance with MD and Handbook 2.3 requirements.

As a result, the agency cannot determine if vendor charges are accurate and fails to control the use of telecommunications services by employees and contractors.

Calling Card Is Not Used Consistently Agencywide

Many employees do not use the Government calling card to make permitted phone calls home while on official travel although the calling card is the agency's preferred vehicle for making these calls. This failure to rely on the calling card occurs because OIS has not been effective in communicating the preference for calling card use to employees and because NRC allows an alternative but more costly means for calling home. As a result, NRC is needlessly spending roughly $31,600 per year more than is necessary to pay for travelers' telephone calls home.

Secure Cell Phone Coverage Is Unreliable

NRC secure cell phone users may not be receiving the best domestic secure cell phone coverage available today. This is because NRC opted to purchase cell phones and service that allow international coverage even though this may not be the best choice for domestic coverage. As a result, these cell phones have failed to provide connectivity in several situations where users wanted secure calling capability. NRC needs to reevaluate available options and allow users to select the option that best meets their coverage and service needs.

Unsecured Telephone Closets in Headquarters and at Technical Training Center

Auditors found unsecured telephone equipment closets at NRC headquarters and at the Technical Training Center. In headquarters, three telephone closets were found either unlocked or opened. This was because NRC has not effectively enforced the requirement to keep the doors locked and has not clearly conveyed to security guards the requirement to check these doors daily. At the Technical Training Center, the telephone closet is not secured

because managers allowed the telephone closet to remain behind an unlocked bi-fold closet door. In either case, agency telephone systems and other equipment maintained in these locations are vulnerable to tampering.

RECOMMENDATIONS

A consolidated list of recommendations appears on pp. 25-26 of this report.

AGENCY COMMENTS

During an exit conference held May 18, 2005, the agency generally agreed with the findings and recommendations in this audit report and provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

[Page intentionally left blank.]

ABBREVIATIONS AND ACRONYMS

FTS	Federal Telecommunications System
GSA	U.S. General Services Administration
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OIG	Office of the Inspector General (NRC)
OIS	Office of Information Services (NRC)
PBX	private branch exchange
TTC	Technical Training Center
WITS	Washington Interagency Telecommunications System

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

NRC's telecommunications program is fundamental to the agency's mission to protect public health and safety and the environment while maintaining an open regulatory process. It is essential that NRC staff have dependable tools and services to enable communication internally and with government and industry officials 24 hours a day, 7 days a week. In this way, NRC can also ensure that important information is communicated to the public in an effective, efficient, and timely fashion.

Telecommunications Program

NRC's telecommunications program is composed of all NRC telecommunications systems, including local and long-distance voice services, voicemail, videoconferencing, and personnel communications equipment (e.g., calling cards, cell phones). OIS provides overall guidance and direction for the agency's regular (i.e., non-secure) telecommunications systems and equipment. The Office of Nuclear Security and Incident Response manages NRC's secure telecommunications systems and equipment. This audit focused primarily on the agency's non-secure telecommunications systems, although auditors also reviewed the agency's use of secure cell phones.

Program management and oversight for the agency's non-secure telecommunications systems and equipment is largely decentralized. Headquarters provides operational and administrative support for its systems and services, and the regions oversee most aspects of their telecommunications programs. An exception is long-distance service, which headquarters manages for the entire agency. In headquarters, the Infrastructure and Computer Operations Division, Computer Operations and Telecommunications Branch, OIS, provides telecommunications support and oversight. In each regional office, the Information Resources Branch provides this function.[1] Region II provides support and oversight for the Technical Training Center.

[1] In Region IV, this office is the Information Resources and Management Branch.

NRC headquarters, regional offices, and the Technical Training Center have different local service contracts, but share the same contract for long-distance service. Local telephone service for headquarters is provided through the Washington Interagency Telecommunications System contract (WITS2001) with the General Services Administration (GSA). Each region and the Technical Training Center has procured its own local telephone service with providers in its vicinity. Agency long-distance service is provided through the Federal Telecommunications System contract (FTS2001) with GSA.

OIS staff are working to revise Management Directive (MD) and Handbook 2.3, *Telecommunications*, dated January 22, 1993. MD and Handbook 2.3 provide agencywide policies and procedures for use of the agency's telecommunications infrastructure. OIS managers decided not to finalize the revision until completion of this audit to ensure that the updated telecommunications guidance addresses issues raised in the audit report.

Computerized Telephone Switches

Headquarters and the regions have different levels of control over the telephone switches used to manage their calls. These switches are of two different types, one a private branch exchange (PBX) and the other a Centrex. Both systems are computer-based devices that can be thought of as small telephone companies. A telephone switch includes a computer processor with memory that allows the owning entity's telecommunications staff to manage telephone call transfers. The PBX is usually housed and maintained by the owning entity (e.g., Government agency, company) specifically for its own use as in the case of regional offices I and III. The Centrex switch is usually housed and maintained by the local telephone company and services many customers.

A Centrex telephone switch, owned and operated by Verizon, under a contract with GSA, allows GSA to manage telephone calls to and from Headquarters. Telephone lines are run by the service provider from the offsite switch to the headquarters buildings' main telephone demarcation rooms to service the offices within. These lines are then extended from the lower level demarcation rooms vertically to telephone closets located on all floors of each building, excluding the lobby level, using building cable which is maintained by the NRC telecommunications staff. These extensions are then run horizontally from the closets to specific office spaces where the corresponding telephone numbers are assigned.

Regions I, III, and IV own and maintain their telephone switches. Region II has use of a GSA telephone switch as part of its office space lease agreement. The Technical Training Center (TTC) uses GSA-provided Centrex service from a telephone switch owned by the Bell South telephone company.

According to the National Institute of Standards and Technology, PBX switch protection is a high priority because unprotected PBX switches make users susceptible to toll fraud, disclosure of sensitive information through eavesdropping, and inconsistent service. The Department of Homeland Security issued a Homeland Security Information Bulletin on June 3, 2003, to alert PBX users about an increase in the number of compromised PBXs and telephone voice mail systems. The bulletin warns users that these intrusions allowed unauthorized users to make long-distance domestic and international telephone calls at the PBX owner's expense. The intruders were also able to make similar connections to Internet service providers.

FY 2003 and FY 2004 Telecommunications Costs

FY 2003 and FY 2004 telecommunications costs for headquarters and the regions are displayed in the following table.

Telecommunications Costs		
Locations	**FY 2004**	**FY 2003**
Headquarters	$5,028,000	$5,824,000
Region I	229,000	155,000
Region II	317,000	335,000
Region III	217,000	257,000
Region IV	306,000	352,000
TTC	42,000	43,000
Total	**$6,139,000**	**$6,966,000**

Headquarters costs include agency long-distance charges and charges for local phone service, voicemail, voice/data infrastructure and support, cell phones, pagers, videoconferencing, and the NRC Message Center services provided by headquarters operators. Regional costs include local and resident site dial tone charges, cell phones, pagers, and other items, but do not include long-distance charges as these are paid for by headquarters.

Cell Phones

OIS pays for and manages most of the cell phones issued to headquarters employees for business purposes, and each region pays for and manages the cell phones it issues to its employees. NRC is currently exploring a plan to reimburse employees for official use of personal cell phones. On November 16, 2004, the Office of General Counsel stated it had no legal objections to a recent proposal submitted jointly by OIS and the Office of the Chief Financial Officer on this subject. According to the proposal, NRC is considering to offer three service level plans to designated employees. Service plan assignments would be based on the agency's determination of the minimum service level each employee would need to fulfill his or her job duties.

Secure Cell Phones

The Office of Nuclear Security and Incident Response manages the agency's secure telecommunications systems and equipment, including secure cell phones. During FY 2002 and FY 2003, officials from that office purchased 20 secure cell phones at a total cost of approximately $43,580. Service costs for these phones totaled approximately $19,600 in FY 2004 and are expected to be similar during FY 2005. Between January and February 2004, the office purchased 20 more secure cell phones.

II. PURPOSE

The audit objectives were to evaluate (1) controls over the use of NRC telecommunications services and (2) the physical security of NRC telecommunications systems. Appendix A contains information on the audit scope and methodology.

III. FINDINGS

Improvements are needed to strengthen controls over the use of NRC's telecommunications services and the physical security of NRC telecommunications systems. Specifically, NRC should

- Improve headquarters oversight of telecommunications services with regard to billing reviews, use of agency toll-free numbers, and telephone line and circuit inventories.
- Ensure more consistent use by travelers of the FTS calling card for long-distance calls.
- Provide additional service options for the agency's secure cell phone users to improve coverage.
- Enforce physical security requirements pertaining to telephone equipment closets.

A. Telecommunications Services Oversight Is Inadequate

OIS telecommunications program oversight does not ensure that employees and contractors are using NRC's telephone system appropriately and that phone bills are accurate. Specifically,

1. OIS performs subjective and limited billing reviews that do not fulfill the requirements in MD and Handbook 2.3.
2. OIS does not conduct sufficient inventories to ensure that all phone lines and circuits for which NRC pays each month are used and necessary.
3. OIS does not restrict use of the headquarters toll-free number in accordance with MD and Handbook 2.3 requirements.

As a result, the agency cannot determine if vendor charges are accurate and fails to control the use of telecommunications services by employees and contractors.

A.1 Headquarters Billing Reviews Do Not Meet Requirements

Billing Review Guidance

MD and Handbook 2.3 contain various provisions for a cost-effective telecommunications program. These provisions require (1) employees to use Government telecommunications services responsibly and in

accordance with requirements, (2) managers to provide oversight to ensure that services are used appropriately, and (3) OIS staff to conduct billing reviews to ensure that costs align with services received.[2] MD and Handbook 2.3 provisions:

- Prohibit employees from making personal long-distance and international calls at the Government's expense.

- Limit employee use of Government telephone systems to official business and certain limited unofficial purposes (e.g., brief, infrequent personal calls that could not reasonably be made at another time).

- Require regional administrators and headquarters office directors to review and validate records of long-distance calls provided by OIS and initiate administrative action to collect reimbursement for unofficial calls.

- Require OIS to conduct a monthly review of telephone call detail records to improve use of the telephone system and reduce overall cost.

- Require OIS to randomly sample cell phone bills on a monthly basis and forward the bills to the appropriate office director for approval.

Billing Reviews are Limited

OIS performs subjective and limited billing reviews that do not fulfill the requirements in MD and Handbook 2.3. As noted in the Background section of this report, OIS oversees local service for headquarters and long-distance service for the entire agency.

OIS staff responsible for examining the local and long-distance bills employ subjective methods for their review and said the bills are difficult to review in depth because they are voluminous.[3] These staff said they rely on their experience and general knowledge of the telecommunications program to determine if monthly charges appear reasonable, but that it is difficult to know for certain that the charges are appropriate. They said they consider cost trends and

[2] MD and Handbook 2.3 assign this and other telecommunications responsibilities to the Office of the Chief Information Officer. This office was renamed on February 1, 2005, to the Office of Information Services.

[3] OIG reviewed local and long-distance bills from October 2002 through September 2004 and noted that these bills, which do not reflect cell phone calls, are composed of thousands of individual calling charges as well as various service costs that vary from month to month. During this time frame, local charges for headquarters averaged $68,761.33 per month and agency long-distance charges averaged $105,212.79 per month.

large variations in monthly cost. They contact vendors to learn why such changes occur and seek bill adjustments, if appropriate. However, the staff do not use any specific benchmarks – or dollar amounts – to alert them when a monthly bill appears questionable. Instead, they review only those charges that they subjectively determine to be questionable, and they do not review call detail records to identify questionable usage by employees and contractors. In addition, they do not provide long-distance call detail records to regional administrators and office directors as required by MD and Handbook 2.3.

Furthermore, OIS staff make no specific effort to review international calls to assess whether employees are making such calls appropriately. Information on international calls is included in the long-distance monthly bills, but staff do not review these records. Compounding this is the fact that headquarters operators place international calls whenever requested by headquarters staff. The operators are not required to ascertain whether the calls are for official purposes and have never challenged a request for an international call. Although the operators maintain a handwritten log of international calls, no one reviews the log to assess whether these calls are legitimate.

In addition, OIS managers do not randomly sample cell phone bills on a monthly basis and provide the bills to office directors, as required by MD and Handbook 2.3. OIS receives support from a contractor tasked to review the headquarters cell phone bills for trends and make recommendations for cost-effective service plan adjustments. However, the contractor does not look for possible misuse of services and only inconsistently fulfills requests from offices to provide their bills for review on a monthly basis.

OIS Lacks Computer Software for Improved Approach

OIS performs subjective and limited billing reviews because OIS management (1) does not require staff to adhere to the requirements in MD and Handbook 2.3 and (2) believes OIS lacks the computer software for a more rigorous approach. Furthermore, as currently written, the draft revision of MD and Handbook 2.3 will be inadequate to ensure an appropriate level of control over the program.

OIS telecommunications managers did not require adherence to the MD and Handbook 2.3 bill review requirements partly because they were unaware that current bill review practices were not in alignment with agency requirements. However, they also defended

the current approach, noting that in the years since the guidance was approved, local and long-distance rates have dropped, making time-consuming reviews of call detail records less necessary than in the past. They said it is primarily up to agency managers to ensure that employees are not misusing the phones (e.g., spending inordinate amounts of time making personal phone calls while at work). OIG finds it illogical that OIS would impose this expectation on managers without providing the resources (i.e., call detail records) needed to perform the task. If agency managers are to ensure employee accountability with regard to telephone usage, it is essential that managers receive the call detail records for their offices on a regular basis.

The OIS managers said that although they would prefer a more rigorous review process, they lack telecommunications billing review software[4] to perform indepth bill reviews each month or to provide office directors and regional administrators with the call detail records for their jurisdictions. Without computer software, they said, manual efforts are too cumbersome and would not be cost-beneficial. OIS managers said they have actively pursued the purchase of such software even prior to the start of this audit.

In addition, as currently written, the proposed draft revision of MD and Handbook 2.3 will be inadequate to ensure the necessary level of control over employee use of telecommunication services. OIG reviewed the draft and noted that it contained weaker oversight provisions than those in the existing guidance. For example, the draft revision of MD and Handbook 2.3 requires office directors and regional administrators to review and validate records of usage provided by OIS and initiate administrative action to collect reimbursement for unauthorized usage, but only "where appropriate and economically feasible." The current version of MD and Handbook 2.3 does not contain this type of caveat and therefore assures more control over employee use of the services. Similarly, the draft version requires OIS to provide information on usage "when appropriate and economically feasible."

[4] Various companies provide telecommunication expense management solutions that allow Federal agencies to proactively manage, optimize, and validate their telecommunications infrastructure and bills. Typically, this involves downloading or inputting charges into an automated database to facilitate review and then running reports to assess whether charges are appropriate and accurate. Vendors claim these solutions are extremely cost-beneficial and more than pay for themselves in costs recouped by users.

Inappropriate Usage and Charges Not Identified

As a result of the existing subjective and limited billing review process, NRC lacks assurance that vendor charges are appropriate and accurate and fails to ensure appropriate use of telecommunications services by employees. Because long-distance and local call detail records are not reviewed, it is easy for employees and contractors to misuse the agency's telecommunication resources. As an example of inadvertent misuse, auditors identified that 5,855 local long-distance calls were made between December 2, 2002, and July 28, 2004, from NRC's voicemail system to a contractor's unused pager. These calls cost NRC $751.71. While this figure is minimal in comparison with the agency's telecommunications budget, it makes clear that NRC's billing review process is ineffective to identify a large number of unwarranted calls and suggests that other potential cases of wasted expense could be overlooked.

A.2 Routine Telephone Line and Circuit Inventories Are Not Conducted

Inventory Requirements

Routine inventories of telephone lines and circuits for which NRC pays a recurring monthly charge are essential to ensure that all these lines and circuits are used and necessary.[5] Although MD and Handbook 2.3 require NRC to conduct annual physical inventories of telecommunications equipment for which the agency pays a recurring charge to assure that vendor billing invoices tally with existing equipment, there is no similar requirement to inventory agency phone lines and circuits, which are viewed as services and not equipment.

Routine Inventories Are Not Conducted

OIS does not conduct routine inventories of the 5,388 phone lines and approximately 54 circuits that run through headquarters and for which NRC pays recurring monthly charges. According to an OIS staff member responsible for managing the headquarters telephone lines and circuits, the last thorough inventory of telephone lines was conducted about 4 or 5 years ago. This inventory did not include a review of telephone circuits. According to the OIS staff member,

[5] According to an OIS staff member, telephone lines are used primarily to carry voice service, while telephone circuits are high-capacity conduits with greater bandwidths and speeds used to support data communications for systems such as internetwork communications or videoconferencing.

monthly charges for individual telephone lines range from about $7.50 to $17, while the charge for individual circuits ranges from about $200 to $2,000 per month. During FY 2004, NRC incurred costs of $731,367.21 for headquarters telephone lines. The amount spent on circuits during the same period is unknown to OIS, according to the OIS employee. Based on the figures the OIS employee provided (approximately 54 circuits, costing NRC between $200 and $2,000 apiece per month), OIG estimates that NRC spent at least $130,000 for telephone circuits during FY 2004.

While the OIS staff member continually tracks changes and additions to telephone lines by updating a database with this information, there is no comparable database of telephone circuits. In addition, no proactive effort is made to identify telephone lines or circuits that are no longer in use or needed by the agency. Lines and circuits become unused when, for example, a system connection is terminated or an employee leaves the agency. Without conducting inventories of the telephone lines and circuits, the staff member said, there is no assurance that NRC is using all the services for which it pays. Furthermore, the staff member said, OIS does not know exactly how many circuits NRC has or the exact amount it pays for these connections.

Inventory Requirements Are Needed

NRC is not conducting routine inventories of NRC telephone lines and circuits because there is no requirement to do so. Telecommunications staff agreed with OIG that routine inventories of the telephone lines would be a good business practice and a means to ensure that NRC is paying for needed services only; however, they said they lack the resources to perform such inventories and to review usage records to identify unused circuits and telephone lines.

Accuracy of Bills Is Unknown

Without conducting routine inventories of telephone lines and circuits, the agency cannot know whether its telephone bills accurately reflect the services for which the agency pays month after month.

A.3 Headquarters Does Not Restrict Use of Its Toll-Free Number

Guidance on Toll-Free Numbers

NRC headquarters and regional offices provide toll-free numbers to their staff to use while on travel. According to MD and Handbook 2.3, the headquarters "800 service" (toll-free number) is to be used by travelers to contact their offices.

MD and Handbook 2.3 are silent concerning regional office use of their region's toll-free numbers, but state that the directive and handbook must be followed by all headquarters and regional employees.

Headquarters is responsible for paying for all of NRC's long-distance charges, including calls made via the toll-free numbers. During FY 2004, NRC paid $40,668 for toll-free calls. According to an OIS official, this total was based on a rate of 2 cents per minute of use.

Headquarters Usage Does Not Match Guidance

While each of NRC's four regional offices restricts use of their toll-free numbers primarily to calls terminating at their offices, this is not the case in headquarters. In headquarters, toll-free calls are answered by NRC operators, who connect callers with numbers inside and outside of headquarters. Operators said they were permitted to connect travelers with their homes as well as headquarters numbers, but stated that many requested connections are not to home or headquarters numbers. They said they sometimes ask callers for their badge numbers to ensure they are speaking with an NRC employee. They also may inquire about the call's purpose to assure that it is for official business. However, they said they would not turn down a connection request.

In three of the regional offices, however, toll-free number calls are connected only to numbers within the regional offices. Subsequently, even employee requests to be connected to an NRC resident inspector at a nuclear power plant would be denied. In the remaining region, toll-free callers are connected to regional office numbers and to licensee sites, but not to any other numbers.

Policy Not Enforced

Headquarters operators connect toll-free callers to numbers outside of headquarters because OIS management has not required operators to enforce the MD and Handbook 2.3 requirements. However, OIS managers expressed differing views on whether this practice was appropriate. Two managers said this practice should be allowed because there are occasions where travelers may need to get in touch with non-headquarters numbers for official purposes. They said using the toll-free number in this manner is sometimes the most cost-effective way to facilitate local and long-distance calling. For example, it may cost NRC less for operators to connect long-distance callers to numbers outside of headquarters than for callers to use the commercial telephones in their hotels. A different manager disagreed and said travelers should use the FTS calling card (see page 14 for description) to make long-distance calls and not go through the operators. This manager pointed out that the toll-free connections cannot be tracked to ensure they were made for official business purposes, while calling card usage can be reviewed.

Agency Cannot Ensure Official Usage

By permitting headquarters operators to freely connect toll-free callers to local and long-distance numbers outside of headquarters, OIS cannot ensure that the service is being used for official agency business only. NRC could be incurring charges for toll-free connections made for unofficial purposes and has no way to assess whether this is so. While there may be circumstances where headquarters and regional toll-free callers should be permitted to make outside connections, these circumstances need to be well-defined and oversight and enforcement need to be performed.

Summary

NRC needs to ensure that employees and contractors are using NRC's telephone system appropriately and phone bills accurately reflect services received. By improving its billing review methods, updating inventory requirements, and clarifying and enforcing its policy concerning usage of its toll-free numbers, NRC will increase its control over telecommunications services and their cost agencywide.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Purchase and implement billing review software to assist in implementing a cost-effective, comprehensive telecommunications billing review process.

2. Establish benchmarks for determining if telecommunications charges are accurate and appropriate.

3. Revise MD and Handbook 2.3 to include effective management controls over headquarters staff use of agency telecommunications services.

4. Establish requirements for routinely conducting inventories of telephone lines and circuits for which the agency pays monthly recurring charges, assessing usage of these telephone lines and circuits, and making adjustments to account for unneeded telephone lines and circuits.

5. Define and enforce appropriate use of agency toll-free numbers.

B. Calling Card Is Not Used Consistently Agencywide

Many employees do not use the Government calling card to make permitted phone calls home while on official travel although the calling card is the agency's preferred vehicle for making these calls. This failure to rely on the calling card occurs because OIS has not been effective in communicating the preference for calling card use to employees and because NRC allows an alternative but more costly means for calling home. As a result, NRC is needlessly spending roughly $31,600 per year more than is necessary to pay for travelers' telephone calls home.

Calling Card Guidance

According to MD and Handbook 2.3, long-distance service via the FTS network should be used to avoid excessive telephone call expense whenever practicable. One feature of the FTS long-distance contract is the Government calling card, which allows employees to make long-distance calls without operator assistance through the FTS network while on official travel. Employees may use the cards while on official travel to make business calls and to make brief calls to their families. The FTS calling card is similar to commercial calling cards in that employees may dial in to the service from any commercial telephone, enter a code, and then dial the number to which they wish to be connected. According to OIS managers, long-distance calls made using the calling card cost the same (2 cents per minute) as all long-distance calls made over the FTS network.

Information concerning calling card use also appears in some regional policies and in hardcopy headquarters telephone directories. For example, Region IV guidance directs that all official calls from outside the office should be made using the Government calling card. Region III guidance encourages staff to use the card when making personal calls home in lieu of toll calls, calls billed to hotel rooms, or collect calls while on travel status.

Although the calling card is the preferred method of long-distance calling for employees on travel, MD and Handbook 2.3 also note that employees traveling for 2 or more nights on Government business may be reimbursed up to $4 per day for a brief (defined as "approximately 5 minutes") call home.

The current revised draft of MD and Handbook 2.3 does not offer the $4 per day option, but allows employees traveling and incurring lodging costs a brief (defined as "not to exceed 30 minutes per day") call per day to their residence, preferably using the calling card.

Calling Card Use Not Consistent

Many NRC employees are not using the Government calling card to call home while on travel and are instead requesting reimbursements for calls made while they are on travel status. OIG auditors reviewed 1,123 travel vouchers processed by the Office of the Chief Financial Officer during September 2004 and found that the agency was paying an average of $147.50 each day to reimburse travelers for phone calls home. The $147.50 was composed primarily of $4 per day charges.[6] Based on this review, auditors estimated that NRC could save about $31,600 each year by requiring travelers to use the Government calling card wherever possible.[7]

Furthermore, there is no documentation to ensure that employee $4 per day claims for calls home reflect actual use. However, long-distance call detail records do track calling card use and therefore provide a means of ensuring accountability by users.

Better Communication Needed

OIS has not effectively communicated to employees the agency's preference for calling card use for calls made home while on official travel. Furthermore, NRC allows employees an alternative way to call home that is more costly.

While OIS has issued 1,413 calling cards to employees, not all travelers possess them and the office does not actively advertise their availability. According to an OIS staff member, in the past, information concerning calling card availability was conveyed to

[6] While most employees claimed $4 per day for calls made home while on travel, a limited number claimed amounts less than $4.

[7] Auditors derived the $31,600 figure by multiplying $147.50 by 252 (i.e., average number of working days per year) and then multiplying the total by 85 percent. This reduction was made to allow for the fact that the revised MD and Handbook 2.3 anticipate that travelers will make 30-minute calls home each day, which, at a rate of 2 cents per minute, would cost the agency about $.60 per day of travel. Use of the calling card would allow the agency to save about 85 percent of the $4 it now pays out for a call home each day of travel.

office information technology coordinators (who are responsible for making requests to OIS for calling cards) in the past. However, information on calling cards has not been conveyed recently to information technology coordinators.

Furthermore, OIS has not tried other methods to inform employees about calling cards. Such methods could include placing notices about calling card availability at the headquarters travel office or alerting Office of the Chief Financial Officer staff to notify employees whose vouchers include $4 per day reimbursement requests that the calling cards are available.

Finally, even if travelers are aware of the calling card option, they may not make the effort to acquire a card because NRC allows all employees the option to submit $4 per day telephone claims.

NRC Is Spending More Than Necessary

By not requiring employees to use the Government calling card to make appropriate calls home while on official travel, NRC is spending approximately $31,600 per year more than necessary. The agency also misses an opportunity to collect call detail information on these calls to ensure that charges are appropriate. OIS needs to (1) take a proactive approach and inform employees about the availability and benefits of using the calling cards and (2) require use of the cards by employees in most travel situations. Exceptions could be made for infrequent travelers.

Recommendations

OIG recommends that the Executive Director for Operations:

6. Develop and implement a communications plan to better inform employees about the availability and benefits of using calling cards.

OIG recommends that the Chief Financial Officer:

7. Discontinue the $4 per day reimbursement option and issue calling cards instead.

C. Secure Cell Phone Coverage Is Unreliable

NRC secure cell phone users may not be receiving the best domestic secure cell phone coverage available today. This is because NRC opted to purchase cell phones and service that allow international coverage even though this may not be the best choice for domestic coverage. As a result, these cell phones have failed to provide connectivity in several situations where users wanted secure calling capability. NRC needs to reevaluate available options and allow users to select the option that best meets their coverage and service needs.

Secure Cell Phones

According to MD and Handbook 12.4, *NRC Telecommunications Systems Security Program*, classified or sensitive unclassified voice telecommunications should be transmitted over protected systems to the maximum degree possible. As part of this program, the agency has a limited number of secure cell phones to facilitate secure conversations from locations where secure telephones are unavailable.

The National Security Agency approves all cryptographic systems and techniques used by the Federal Government. Therefore, according to an employee from the Office of Nuclear Security and Incident Response (NSIR), the National Security Agency certifies the secure cell phone technology and agencies must purchase phones and services that use the certified technology.

MD and Handbook 12.4 predate the agency's purchase of secure cell phones and do not specifically address this type of equipment. OIG presumes, however, that NRC expects these cell phones to offer the best coverage in as many locations as possible so that they can facilitate connectivity whenever and wherever needed.

Furthermore, according to an NSIR employee, when the agency initially purchased the secure cell phones, the intent was that employees would use the secure cell phone as their main NRC cell phone because the phone offers both secure and regular communication capabilities.

Many Users Are Dissatisfied With Coverage

NRC secure cell phone users may not be receiving the best secure cell phone coverage available today. OIG surveyed 19[8] employees to whom secure cell phones were assigned and learned that most were either dissatisfied with the coverage, unaware about coverage because they had not tested it, or felt the coverage was inferior to that offered by their regular cell phone. Only 3 of the 19 used the secure cell phone as their primary agency cell phone. Of the 16 who did not use the secure cell phone as a primary phone, 15 had a second agency cell phone that they used as their primary business cell phone. The 16th employee opted to use a personal cell phone for official business. Reasons provided for not using the secure cell phone as a primary phone included problems with coverage, concern over losing or damaging the secure cell phone, and the perception that the cell phones were for emergency use only.

In general, regional users were less aware of and less satisfied with secure cell phone coverage than headquarters users. Only three of five regional users had tested coverage of the secure cell phones, and only one believed the coverage was comparable to the employee's regular cell phone. Of 11 headquarters users, 7 had tested coverage and 4 thought the coverage was comparable to their regular cell phone. Of the 19 users, 6 shared their knowledge of dead spots with other users and 1 documented this information to share with others. Of those surveyed, only 2 had made an international call. A third person had tried unsuccessfully to make such a call.

NRC recently purchased an additional 20 secure cell phones, costing $2,179 apiece, to use in headquarters and the regions.

International Capability Has Impact On Domestic Coverage

Some secure cell phone users may not be receiving the best coverage domestically because NRC opted to purchase phones and service that allow international coverage – even though these may not be the best choices for domestic coverage. According to staff who were involved in the selection process in 2002, a primary

[8] At the time the survey was conducted, NRC had assigned 20 phones to 19 employees (1 employee was assigned 2 phones). Of the 20 phones, 12 were assigned to headquarters employees and 8 to regional employees.

factor was the interest by several individuals in being able to make international calls. However, 16 of 19 NRC secure cell phone users have never attempted to place an international call with these phones and consequently failed to benefit from this feature.

Because NRC opted for secure cell phones and service that may not be the best choice for domestic coverage, the phones failed to work during several emergency exercises. During these exercises, users were not successful in making desired connections even though in at least one case the employee's regular cell phone could make the connection. In an additional example of phone failure, an employee could not get coverage using the secure cell phone during a hurricane.

Coverage Could Be Improved

By selecting service plans for the regions and headquarters that provide the best coverage for users in these different geographic locations, NRC can better ensure that the secure cell phones provide connectivity when needed. Furthermore, NRC should not purchase any additional secure cell phones without evaluating whether it would be advantageous to select phones that do not allow international coverage, but which provide better coverage domestically.

Recommendations

OIG recommends that the Executive Director for Operations:

8. Select secure cell phone service plans for the regions and headquarters that provide the best coverage for users in these different geographic locations.

9. If additional secure cell phones are purchased, select phones that will facilitate the best coverage for users in the regions and in headquarters.

D. Unsecured Telephone Closets in Headquarters and at Technical Training Center

Auditors found unsecured telephone equipment closets at (1) NRC headquarters and (2) the Technical Training Center. In headquarters, three telephone closets were found either unlocked or opened. These headquarters closets were unsecured because NRC has not effectively enforced the requirement to keep the doors locked and has not clearly conveyed to security guards the requirement to check these doors daily. At the Technical Training Center, the telephone closet is not secured because managers allowed the telephone closet to remain behind an unlocked bi-fold closet door. In either case, agency telephone systems and other equipment maintained in these locations are vulnerable to tampering.[9]

D.1 Headquarters Closets Were Found Unsecured

Security Requirements

NRC's telecommunications systems are subject to the physical security controls required by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." These physical security requirements, detailed in MD and Handbook 12.5, *NRC Automated Information Security Program*, specify that telephone and wiring closets should be kept locked at all times when unattended and that access should be restricted to a limited number of accountable personnel.

National Institute of Standards and Technology publications also emphasize the importance of physical security controls to prevent unauthorized access to telephone closets and PBX facilities. According to the *Federal Agency Security Practices Agency IT Security Handbook*, telephone-wiring closets should be kept locked and secured. National Institute of Standards and Technology requirements state that telephone closet doors should be secured with a cipher lock or suitable substitute at a minimum.

Three Headquarters Closets Were Unsecured

NRC headquarters telephone equipment closets were left unsecured and unattended in several locations in the NRC headquarters buildings.

[9] Auditors also reviewed physical security measures employed in the regions to protect their telephone switches. Appendix B contains information on these security practices.

Despite requirements to keep the telephone closets secured when unattended, OIG found three unsecured doors during a physical security inspection. These closets contain badge system wiring, air conditioning components, and other equipment.

On December 14, 2004, the audit team performed an inspection of the 43 telephone closets and 2 telephone equipment rooms in the One and Two White Flint North headquarters buildings to ensure that the telecommunications equipment was protected from unauthorized access. Auditors noted that while each of the doors protecting these areas had access control features,[10] two telephone closet doors in the One White Flint North building were unlocked because the override buttons were enabled, preventing the bolt from releasing to lock the doors. Auditors also found that a telephone closet door in the Two White Flint North building was left open for more than 2 hours on the day of the inspection. Auditors checked this closet several times over the 2-hour period and noted that no one was working inside or nearby. Furthermore, this closet had been seen open and unattended on several prior occasions.

According to an OIS official, telecommunication contractors are instructed to lock the telephone closet doors whenever their work has been completed or they step out of the line of site of the doors. This official said that the contractors are also reminded of this policy whenever security guards inform OIS staff that security guards found telephone closets unlocked during their security checks. OIG notes that it is difficult at times to identify a specific individual responsible for leaving the closets unlocked and unattended because the closets are accessed by both telecommunications and Division of Facilities and Security contractors.[11] However, the telecommunications services contract requires contractors to adhere with NRC security requirements to keep the telephone closet doors shut.

[10] Cipher locks are used to control access to the One and Two White Flint North telephone equipment closets. The headquarters badge access control system controls access to the two telephone equipment rooms. These rooms have this added level of access control because they serve as the entry point for headquarters' 5,388 telephone lines, which are used for employee telephones, fax machines, modems, remote access to building management and security systems, video and audio conferencing systems, computer systems, and systems for the hearing impaired.

[11] Division of Facilities and Security contractors require access to the closets to perform work on the headquarters badging system and air conditioning, which also run through the telephone closets.

OIS Lacks Enforcement Method

Headquarters NRC telephone equipment closets were left unsecured because OIS lacks a method for ensuring that contractors follow the security policy to keep the telephone closet doors locked. Furthermore, the Office of Administration has not provided clear guidance to NRC security guards on their responsibility to routinely check these doors while conducting patrols.

Although telecommunications contractors are reminded to lock the telephone closet doors, and it is a contract requirement, OIS lacks a method of enforcing this measure. OIG discussed this situation with Office of Administration officials and learned that NRC could issue contractors security infractions for leaving the doors unlocked. A security infraction is an administrative action that NRC takes when an employee or contractor fails to comply with NRC security requirements. The issuance of three security infractions to any one contractor could result in the loss of his or her ability to work as a contractor at NRC. The telecommunications contract would need to be modified to note enforcement of security policies and the issuance of security infractions when telephone closet doors are found unsecured. OIG also learned that NRC could fine contractors for leaving the doors unsecured, provided the contract is modified to include such a provision.

NRC's security guard contract requires roving security guards to check doors throughout the facility to ensure they are locked. However, the post order for roving guards does not state this specifically, which weakens the agency's assurance that these checks are occurring consistently and routinely. The post order directs guards to check the computer room doors, but does not mention the telephone closets. An Office of Administration official said the computer closet check was specifically added to the post orders because the guards need to check the temperature of the rooms to ensure they are not too hot. The inclusion of the requirement to check the telephone closet doors will help to ensure the security policies are being enforced.

Security Vulnerability

When any telephone closet door in One or Two White Flint North is left unsecured, the phone system for that particular floor is jeopardized because of how the system is wired. Tampering with

telephone lines can expose the telephone phone switch to penetration by a hacker. Furthermore, the badging and the air conditioning systems are also vulnerable because they are also located in the telephone closets.

D.2 Technical Training Center – Open Access to the Telephone Closet

Security Requirement

As stated previously, MD 12.5 requires that telephone closets be locked at all times and access to the telephone and wiring closets be restricted to a limited number of accountable personnel.

One Closet Is Unprotected

One of the Technical Training Center's telephone equipment closets is not appropriately protected. This closet is located behind an unsecured bi-fold door within a supply room that is kept open during the workday for the convenience of the professors and staff. The closet door has no locking mechanism to control the access to the telephone lines.

Managers Did Not Enforce Agency Policy

The Technical Training Center telephone closet was not protected because managers failed to enforce agency security policy for the protection of telephone and wiring closets.

Closet Is Vulnerable to Tampering

Unauthorized access to the Technical Training Center's telephone closet can allow for tampering and a disruption of telephone service through the manipulation of the telephone lines housed in the telephone closet. As noted previously, tampering can expose the telephone switch to penetration by hackers. While the Technical Training Center's PBX is not located within the center's office suite, it does not diminish the need for the center's managers to protect the telephone lines once they have entered Technical Training Center office space.

Summary

NRC has not effectively enforced its security policy to keep telephone closets locked when unattended. Three telephone closets were found unsecured in the One and Two White Flint

North buildings during a physical security inspection and the telephone closet at the Technical Training Center is not protected by a locking door. Failure to protect telephone lines exposes NRC to toll fraud, disclosure of sensitive information, or the disruption of service because the telephone switch becomes vulnerable to penetration.

Recommendations

OIG recommends that the Executive Director for Operations:

10. Implement the existing security guard contract requirement to ensure the telephone closet doors are checked throughout the facility and add the requirement to check the telephone closet doors to the security guard post orders.

11. Issue periodic written reminders to telecommunications contractors, and to other contractors who require access to the telephone closets, conveying the NRC security requirement to keep the telephone closet doors locked when the closets are unattended.

12. Impose penalties, such as security infractions or fines, on individuals who do not adhere to the security requirement to keep the telephone closet doors locked.

13. Install a locking door on the telephone closet within the Technical Training Center office suite to prevent unauthorized access to the telephone lines.

IV. AGENCY COMMENTS

During an exit conference held May 18, 2005, the agency generally agreed with the findings and recommendations in this audit report and provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

V. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Purchase and implement billing review software to assist in implementing a cost-effective, comprehensive telecommunications billing review process.

2. Establish benchmarks for determining if telecommunications charges are accurate and appropriate.

3. Revise MD and Handbook 2.3 to include effective management controls over headquarters staff use of agency telecommunications services.

4. Establish requirements for routinely conducting inventories of telephone lines and circuits for which the agency pays monthly recurring charges, assessing usage of these telephone lines and circuits, and making adjustments to account for unneeded telephone lines and circuits.

5. Define and enforce appropriate use of agency toll-free numbers.

6. Develop and implement a communications plan to better inform employees about the availability and benefits of using calling cards.

OIG recommends that the Chief Financial Officer:

7. Discontinue the $4 per day reimbursement option and issue calling cards instead.

OIG recommends that the Executive Director for Operations:

8. Select secure cell phone service plans for the regions and headquarters that provide the best coverage for users in these different geographic locations.

9. If additional secure cell phones are purchased, select phones that will facilitate the best coverage for users in the regions and in headquarters.

10. Implement the existing security guard contract requirement to ensure the telephone closet doors are checked throughout the facility and add the requirement to check the telephone closet doors to the security guard post orders.

11. Issue periodic written reminders to telecommunications contractors, and to other contractors who require access to the telephone closets, conveying the NRC security requirement to keep the telephone closet doors locked when the closets are unattended.

12. Impose penalties, such as security infractions or fines, on individuals who do not adhere to the security requirement to keep the telephone closet doors locked.

13. Install a locking door on the telephone closet within the Technical Training Center office suite to prevent unauthorized access to the telephone lines.

Appendix A

SCOPE AND METHODOLOGY

Auditors reviewed NRC's telecommunications program to evaluate (1) controls over the use of NRC telecommunications services and (2) the physical security of NRC telecommunications systems.

Audit work excluded telecommunications associated with incident response operations because this program was the subject of a recent OIG review. Auditors assessed physical security measures employed by headquarters, the regions, and the Technical Training Center to protect their telephone equipment, but did conduct penetration testing on agency telecommunications systems. Penetration testing did not occur because anticipated assistance from a National Security Agency telecommunications expert was unavailable during the audit timeframe.

Auditors reviewed and analyzed Federal guidance, agency directives, and security standards to establish the internal controls over telecommunication services and requirements for the security of the telecommunications system. A review of the draft MD and Handbook 2.3 was performed to provide OIS staff with recommendations for updating the instruction.

Auditors analyzed the feasibility of requiring employees to use calling cards for calls home while on travel instead of claiming a $4 charge per day for 5-minute telephone calls home. Travel reimbursements paid during the month of September 2004 were reviewed to estimate the number of $4 reimbursements claimed for telephone calls and the amount paid by the agency for calls home made by employees on temporary duty travel.

Auditors performed a security inspection of headquarters, regional office, and Technical Training Center telephone equipment rooms and closets to assess protection provided to the telecommunications equipment. Interviews of headquarters, regional office, and Technical Training Center telecommunications staff were conducted to learn about the management and administration of the telecommunications program. In addition, auditors interviewed agency security staff to determine the implementation of security requirements with respect to the telecommunications equipment.

This review was conducted from July 2004 to January 2005 in accordance with generally accepted Government auditing standards. Internal control weaknesses have been noted and considered for reporting. The work was conducted by Beth Serepca, Team Leader; Shyrl Coker, Audit Manager; and Judy Gordon, Audit Manager.

Appendix B

PHYSICAL SECURITY MEASURES FOR REGIONAL PBX SWITCHES

OIG found that each of the regions are implementing the physical security and access controls required by the National Institute of Standards and Technology (NIST) and MD and Handbook 12.5 for the protection of the PBX telephone switches, therefore no recommendations are made in this area. The telephone switches are secured in locked equipment rooms, password controls are exercised, and modems are kept disconnected to prevent unauthorized remote access to the telephone switch. The implementation of these physical security and access controls protects the regions from vulnerabilities associated with the use of unprotected telephone switches such as toll fraud, the theft of proprietary, personal, and other sensitive information as well as eavesdropping.

OIG was unable to perform penetration tests of NRC's telecommunication system because of the unavailability of an expert from the National Security Agency.

PBX Security Requirements

Security measures for PBX systems are issued in NIST Special Publication 800-24 *PBX Vulnerability Analysis*. NIST specifically stipulates that the PBX and its network equipment should be secured to protect it from damage and unauthorized access or use through the use of locked doors, automatic detection devices, and positive identification and authentication controls. NIST guidance further states that access to the PBX should be minimized to include authorized personnel only, and that password management is essential to good security. The passwords themselves should be controlled so that they expire after a period of time. NIST further warns that because PBXs typically require remote maintenance by vendors, remote access should normally be blocked. These physical security and access control measures are included in MD and Handbook 12.5 and are provided on the Federal Agency Security Practices web site for the application of Federal security professionals.

Regions Implemented Protections

The regions have either implemented all of the required PBX protections or are using a PBX managed by another entity that has implemented all of the suggested protections. Regions I, III, and IV have possession of their own PBX telephone switches, and these are directly managed by the regional Information Resources Branch staff. Region II, located in a GSA-leased building, pays for the use of GSA's PBX telephone switch as part of its lease agreement for office space.

Physical Security and Access Controls Implemented

	Maintained in Locked Space	**Password Controls**	**Limited Access to PBX Software**	**Prevent Remote Access**
Regions I, III, and IV	Card access control systems or key used to secure the PBX	Passwords changed every 30 to 90 days	2 to 3 people have access to the PBX software	Modems are physically disconnected
Region II through GSA	Alarmed doors with cameras	Passwords changed periodically in accordance with GSA requirements	Access is limited to GSA telephone technicians and their supervisor	Modems are physically disconnected