U.S. Nuclear Regulatory Commission

Office of the Inspector General

Semiannual Report to

Congress

April 1, 2005 – September 30, 2005

OIG VISION

"We are agents of positive change striving for continuous improvement in our agency's management and program operations."

NRC-OIG MISSION

NRC-OIG's mission is to (1) independently and objectively conduct and supervise audits and investigations relating to NRC's programs and operations; (2) prevent and detect fraud, waste, and abuse, and (3) promote economy, efficiency, and effectiveness in NRC's programs and operations.

Cover photo courtesy of NEI.

Loading spent fuel rods into storage pool at Comanche Peak.

A MESSAGE FROM THE INSPECTOR GENERAL

This Semiannual Report to Congress highlights the activities of the U.S. Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) for the 6-month period ending September 30, 2005.

Before summarizing our recent activities, I want to acknowledge the excellence and competence of the auditors, investigators, and support staff who form the foundation of the NRC OIG. Just recently, for the third consecutive year, two of our audit and investigative teams were recognized by the President's Council on Integrity and Efficiency for outstanding performance. Most recently, the Award for Excellence in Audit was received for significant accomplishment in auditing and reporting on the ability of the NRC to respond to a security incident at United States nuclear power plants. The Award for Excellence in Investigations was received for outstanding work in investigating and reporting failures in the NRC's billing and financial statement process for nuclear reactor plants licensed by the agency. I commend these talented men and women for their hard work and dedication to the mission of this office.

Our office completed 13 performance audit reports of NRC's programs and operations making numerous recommendations to NRC for program improvement. Of note, the audit of NRC's contract closeout process showed that $6.4 million could be put to better use by the timely deobligation of funds on expired contracts. In addition, OIG completed 51 investigations and 2 Event Inquiries. Thirteen cases were referred to the Department of Justice and 19 were forwarded to NRC management for action during this reporting period.

Finally, I would like to express my appreciation for the collaborative work between my staff and agency managers to address OIG findings and implement the recommendations made by my office. I look forward to continuing this work as we strive to accomplish our common goal of ensuring the effectiveness, efficiency, and integrity of NRC programs and operations.

Hubert T. Bell

CONTENTS

Highlights v

OIG Organization and Activities 1

NRC's Mission 1

OIG Mission and Strategies 1

Audit Planning 2

Investigative Activities 3

OIG General Counsel Activities 4

Regulatory Review 4

Training at the Office of Government Ethics Conference 6

Other Activities 7

New OIG Management Information System 7

Attendance at NOBLE Conference 8

NRC OIG Shares Expertise with Frederick County, MD 9

OIG Staff Learn About France's Nuclear Program 10

Audits 11

Audit Summaries 11

Audits In Progress 22

Investigations 26

Investigative Case Summaries 26

Statistical Summary of OIG Accomplishments 33

Investigative Statistics 33

Audit Listings 35

Audit Tables 37

Abbreviations and Acronyms 41

Reporting Requirements 43

HIGHLIGHTS

The following two sections highlight selected audits and investigations completed during this reporting period. More detailed summaries appear in subsequent sections of this report.

AUDITS

- The NRC Reactor Program System (RPS) is an information technology tool that provides planning, scheduling, and reporting capabilities to support the NRC reactor inspection and licensing program. OIG conducted an audit to determine whether the RPS provides for the availability, confidentiality, and integrity of the data stored in the system, and meets its required operational capabilities.

- Camera cell phones, if misused, pose security and privacy threats because they enable people to covertly photograph images or scenes and transmit them immediately to the Internet. OIG conducted an audit of NRC's policy and practices concerning camera cell phones.

- NRC's telecommunications program includes local and long-distance voice services, voice mail, videoconferencing, and personal communications equipment. Although OIG's audit focused primarily on the agency's non-secure telecommunications systems, it also addressed the agency's use of secure cell phones.

- Listed systems that process safeguards and/or classified information require more security protections than the typical unclassified information processing systems. OIG conducted a system evaluation to test the effectiveness of the security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information.

- As part of the audit of NRC's Decommissioning Program, OIG examined aspects of the NRC's approach to applying the Office of Management and Budget's Program Assessment Rating Tool (PART). PART is a diagnostic tool intended to systematically and consistently assess the performance of program activities across the Federal Government.

- OIG conducted an audit to determine whether (1) NRC's contract closeout policies and procedures adhere to applicable regulations, (2) management controls associated with the closeout process are adequate, and (3) NRC complies with its own closeout procedures, with an emphasis on timeliness.

- Decommissioning is defined as removing a nuclear facility or site safely from service and reducing residual radioactivity. OIG conducted an audit to determine whether NRC's Decommissioning Program achieves the desired performance and results as stated in the agency's strategic plan.

- OIG conducted a system evaluation to evaluate the effectiveness of NRC security policies, procedures, practices, and controls for standalone personal computers and laptops.

- NRC's primary means of communicating concerns or issues to licensees is through generic communications. The purpose of this audit was to assess the effectiveness of the agency's generic communications program.

- Consistent with the requirements of the Federal Information Security Management Act (FISMA), OIG conducted a series of assessments to provide NRC with the information needed to determine the effectiveness of its overall information security programs and for it to develop strategies and best practices for improving information security.

- The Reports Consolidation Act of 2000 requires that each Inspector General summarize what he or she considers to be the most serious management and performance challenges facing the agency and assess the agency's progress in addressing those challenges. The NRC IG identified nine management challenges that are considered to be the most serious.

INVESTIGATIONS

- OIG conducted an investigation based on information that NRC Region I should have been aware of underlying equipment and operational problems at the Hope Creek Nuclear Generating Station that surfaced after a drain tank pipe failure.

- OIG completed an investigation based on information that a Federal Government vendor was suspected of double billing, fraudulently adding freight/shipping charges to purchases, and selling non-trade compliant equipment to the Federal Government.

- In response to a Congressional request and allegations from the public, OIG conducted an Event Inquiry to determine the adequacy of NRC's oversight of the Vermont Yankee Nuclear Power Station extended power uprate review process.

- OIG conducted an investigation of a materials licensee in Puerto Rico and the licensee's president for falsely claiming Small Entity Status and obtaining reduced annual license fees from the NRC.

- OIG completed an investigation into NRC's handling of reports that two radioactive sources imported from Russia by a private firm were missing for several months after they cleared customs in New York.

- OIG completed an investigation that determined that an NRC attorney entered Notices of Appearance and represented the NRC in administrative court proceedings before the Atomic Safety and Licensing Board Panel without the required active attorney bar membership.

- During an OIG proactive initiative to review academic credentials of NRC employees, OIG discovered that an NRC employee had listed a fictitious Bachelor of Science degree on an official security form and an application for a promotion.

OIG ORGANIZATION AND ACTIVITIES

NRC's MISSION

The mission of the U.S. Nuclear Regulatory Commission (NRC) is to license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. NRC's scope of responsibility includes regulation of commercial nuclear power plants; research, test, and training reactors; nuclear fuel cycle facilities; medical, academic, and industrial uses of radioactive materials; and the transport, storage, and disposal of radioactive material and waste. NRC's regulations are designed to protect the public and occupational workers from radiation hazards in industries that use radioactive materials.

OIG is committed to ensuring the integrity of NRC programs and operations.

OIG MISSION AND STRATEGIES

In 1978, the United States Congress passed the Inspector General (IG) Act to ensure integrity and efficiency within the Federal Government and its programs. NRC's OIG was established on April 15, 1989, pursuant to Inspector General Act Amendments contained in Public Law 100-504. OIG's mission is to (1) conduct and supervise independent audits and investigations of agency programs and operations; (2) promote economy, effectiveness, and efficiency within the agency; (3) prevent and detect fraud, waste, and abuse in agency programs and operations; (4) develop recommendations regarding existing and proposed regulations relating to agency programs and operations; and (5) keep the agency head and Congress fully informed of problems in agency programs.

OIG is committed to ensuring the integrity of NRC programs and operations. Developing an effective planning strategy is a critical aspect of accomplishing this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, the OIG Strategic Plan for Fiscal Years (FYs) 2003 - 2008 is based, in part, on an assessment of the strategic challenges facing NRC. The plan identifies OIG's priorities and sets out a shared set of expectations regarding the goals OIG expects to achieve and the strategies that will be employed to do so. OIG's Strategic Plan features three goals which generally align with NRC's mission and goals:

1. Advance NRC's efforts to enhance **safety** and protect the environment.

2. Enhance NRC's efforts to increase **security** in response to the current threat environment.

3. Improve the economy, efficiency, and effectiveness of NRC **corporate management.**

Audit Planning

Effective audit planning requires current knowledge about the agency's mission and the programs and activities used to carry out that mission. Accordingly, OIG continually monitors specific issue areas to strengthen OIG's internal coordination and overall planning process. Under the OIG Issue Area Monitor (IAM) program, staff designated as IAMs are assigned responsibility for keeping abreast of major agency programs and activities. The broad IAM areas address nuclear reactors, nuclear materials, nuclear waste, international programs, security, information management, and financial management and administrative programs.

The audit planning process is designed to yield audit assignments that will identify opportunities for efficiency, economy, and effectiveness in NRC programs and operations; detect and prevent fraud, waste, and mismanagement; improve program and security activities at headquarters and regional locations; and respond to unplanned priority requests and targets of opportunities. The priority for conducting audits is based on (1) mandatory legislative requirements; (2) emphasis by the President, Congress, NRC Chairman, or other NRC Commissioners; (3) a program's susceptibility to fraud, manipulation, or other irregularities; (4) dollar magnitude, or resources involved in the proposed audit area; (5) newness, changed conditions, or sensitivity of an organization, program, function, or activities; (6) prior audit experience, including the adequacy of internal controls; and (7) availability of audit resources.

Investigative Activities

OIG investigative strategies and initiatives add value to agency programs and operations by identifying and investigating allegations of fraud, waste, and abuse leading to criminal, civil, and administrative penalties and recoveries. By focusing on results, OIG has designed specific performance targets with an eye on effectiveness. Because NRC's mission is to protect the health and safety of the public, the main investigative concentration involves alleged NRC misconduct or inappropriate actions that could adversely impact on health and safety-related matters. These investigations typically include allegations of:

- Misconduct by high-ranking NRC officials and other NRC officials, such as managers and inspectors, whose positions directly impact public health and safety.
- Failure by NRC management to ensure that health and safety matters are appropriately addressed.
- Failure by NRC to appropriately transact nuclear regulation publicly and candidly and openly seek and consider the public's input during the regulatory process.
- Conflict of interest by NRC employees with NRC contractors and licensees.

OIG has also implemented a series of proactive initiatives designed to identify specific high-risk areas that are most vulnerable to fraud, waste, and abuse. A primary focus is electronic-related fraud in the rapidly developing E-Government processes within NRC. OIG is committed to improving the security of this constantly changing electronic business environment by investigating unauthorized intrusions and computer-related fraud, and by conducting computer forensic examinations. Other proactive initiatives will focus on determining if instances of procurement fraud, theft of property, Government credit card abuse, and fraud in the Federal Employees Compensation Act program are evident.

OIG GENERAL COUNSEL ACTIVITIES

Regulatory Review

Pursuant to the Inspector General Act, 5 U.S.C. App. 3, Section 4(a)(2), OIG reviews existing and proposed legislation, regulations, and implementing Management Directives (MD) and policy issues and makes recommendations concerning their impact on the economy and efficiency of programs and operations administered by the agency. NRC agency directives that require submission of all draft legislation, regulations, and policies to OIG facilitate this statutory review.

OIG conducts its regulatory review program by examining submitted documents reflecting proposed regulatory, statutory, and policy actions and measures them against standards evaluating the potential for fraud, efficiency, and effectiveness. The review also encompasses issues raised in OIG investigations, audits, and prior regulatory review commentaries.

In addition, OIG commentaries are used to address issues related to preserving the independence and integrity of OIG under its statutory precept. These objectives are met through formal memoranda as well as meetings and discussions.

In order to more effectively track agency response to regulatory review comments, the OIG requests written replies within 90 days, with either a substantive reply or status of issues raised by the OIG.

From April 1, 2005, through September 30, 2005, OIG reviewed more than 215 agency documents, including approximately 60 Commission papers (SECYs) and 155 Federal Register Notices, regulatory actions, and statutes.

The most significant commentaries are summarized below:

Management Directive (MD) 3.4, *Release of Information to the Public*, and MD 3.54, *Collection of Information and Reports Management*, both focused on protection of sensitive information with concurrent concern for appropriate openness. For MD 3.4, OIG highlighted a new requirement to perform document security reviews of documents as part of the Sensitive Information Screening

Project (SISP), and proposed that the SISP be included in future drafts. OIG also added language to clarify treatment of its investigative and audit documents and authority to designate documents as Official Use Only. OIG suggestions on 3.54 related advice to more precisely identify the positions responsible for clearance officer approval.

MD 4.2, *Administrative Control of Funds*, MD 4.3, *Financial Management Systems*, and MD 11.6, *Financial Assistance Program*, all related to oversight of agency funding. Extensive comments were issued for MD 4.2, both to reflect the independent role of OIG and to share our office's audit and oversight experience with the agency in this critical area. Our comments focused on reporting requirements in instances of suspected misconduct, with specific directions in the case of potential Anti-Deficiency Act violations. In addition, travel funding and reimbursement issues were highlighted for clarification and obligations and deobligation of funds in procurement actions was discussed with an emphasis on consistency and inclusion of reference to work by the Department of Energy. Similarly, MD 4.3 comments related the need for reference to OIG's role in assisting the agency in cases of alleged or suspected fraud, waste, or abuse. To further this interest, OIG suggested the addition of the IG Act as a reference and specific direction for employees to report suspected wrongdoing to the Inspector General. Our comments on MD 11.6, which described the functions of the Small Business and Civil Rights office in its oversight of funding, suggested more comprehensive guidance to include both pre- and post-award reviews. Additional direction to specify expected timeframes for required actions was also provided.

MD 10.137, *Senior Executive Service Performance Management System*, and MD 10.138, *Senior Executive Service (SES) Reduction In Force (RIF)*, both updated guidance on personnel practices as they pertain to SES employees. MD 10.137, appropriately described the new SES appraisal system. OIG suggested inclusion of the IG Act as a reference to the IG's independent personnel authority over SES staff within the OIG. In addition, consistency in terminology for positions, e.g., "Rating Official," should be used throughout the directive. Under the RIF procedures described in MD 10.138, OIG related the need to separately identify the authority of the IG over SES personnel in the OIG. The need for additional definitions was also identified, along with suggested guidance to include provisions stating that rules applicable to veterans do not apply to SES members.

MD 2.8, *Project Management Methodology*, describes the processes and procedures applicable to information technology (IT) resource management. The matters addressed in the OIG comments included recommendations for more precise identification of agency officials responsible for actions in the IT review and approval process and their respective roles. OIG also suggested that internal software policies be included.

Training at the Office of Government Ethics Conference

On September 20, 2005, Maryann L. Grodin, the General Counsel to the NRC Inspector General, Jerry Lawson, Counsel to the Small Business Administration IG, and Gladis Griffith, Counsel to the U.S. Postal Service Inspector General, presented a panel discussion on "The Relationship Between Designated Agency Ethics Officials (DAEO) and Inspectors General" at the U.S. Office of Government Ethics (OGE) Annual Conference in New York, NY. This panel was part of a 3-day program for more than 500 Federal attorneys.

The presentation focused on aspects of legal areas most relevant to the functions of Inspectors General and DAEOs. Ms. Grodin's presentation described the statutory framework of 5 U.S.C App. 4, the OGE provisions which direct the duties and responsibilities of DAEOs, and 5 U.S.C. App. 3, the Inspector General Act, which is the source of authority for Inspectors General and their staffs to oversee agency programs and operations. Mr. Lawson and Ms. Griffith addressed issues involved in internal investigations and the duty to report suspected violations. In addition to their prepared remarks, each of the panel members fielded questions from the audience on topics ranging from standards of proof supporting the duty to report suspected wrongdoing, Federal fraud statutes, criminal and civil investigative processes, attorney client privilege, and jurisdiction. Case examples were used to illustrate points including sensitive matters of wrongdoing by public officials and cooperation between IG offices and Ethics officials.

OTHER ACTIVITIES

New OIG Management Information System

In April 2005, the NRC OIG implemented the second phase of a new management information system (MIS) designed to enable staff to work smarter and boost efficiency.

Over the years, program requirements to support the OIG's mission changed, but the automated tools used to support OIG business processes did not. OIG systems were standalone, single-user systems, developed with what is now considered to be dated technology. They were difficult to maintain, enhance, and integrate into NRC's information technology architecture, and required the use of many manual processes to compensate for deficiencies. To increase the office's efficiency and effectiveness, OIG initiated a project to implement a modern, multi-user MIS to meet business requirements.

System requirements and potential solutions were identified, alternatives were evaluated, and a business case analysis was prepared. Two commercial-off-the-shelf products developed by Paisley Consulting, *AutoAudit and Magnum Case Management Software*, were chosen as OIG's MIS software solution.

OIG investigative members participating in MAGNUM training. MAGNUM is an integral part of the new OIG Management Information System.

The OIG MIS provides an environment that allows the audit and investigation components to complete their work in shared, secure databases. Users create essential documents in the system, and they are automatically organized into electronic folders by audit or investigation. The shared database design makes documents immediately available to other team members for collaboration, and to managers for review and comment. Built-in workflow and standard format

capabilities ensure that established processes are followed. MIS databases are encrypted, and access is controlled at the database, document, and field levels. Remote access features allow users to work offline and replicate changes back to the central databases.

AutoAudit was implemented in January 2004, and automates key aspects of the audit process. The program provides the ability to assess risk and develop annual audit plans; manage and schedule staff resources; prepare, review, and approve audit work papers; track progress in meeting audit milestones; and track resolution of audit recommendations.

Magnum was implemented in April 2005, and automates key aspects of the investigation process. The program provides the ability to receive and process allegations; create and process investigations; manage and schedule staff resources; prepare, review, and approve investigative documents; track progress in meeting investigation milestones; and track prosecutorial and administrative referrals.

The OIG MIS increased office efficiency by eliminating 3 legacy systems and approximately 20 manual forms, reducing duplicate data entry, enhancing management's ability to supervise and monitor OIG activities, balancing staff workloads, and measuring success based upon established performance measures.

Attendance at NOBLE Conference

NRC OIG staff members, including Inspector General Hubert T. Bell, attended the 29th Annual National Organization of Black Law Enforcement Executives (NOBLE) Training Conference from July 23 -27, 2005, in Atlanta, Georgia. NOBLE was first conceptualized during a 1976 symposium on reducing crime in urban low income areas, sponsored by the Joint Center for Political Studies, the Police Foundation, and the Law Enforcement Assistance Administration. Recognizing the need for black police executives to exchange ideas and opinions about law enforcement and their individual leadership roles in policymaking and establishing law enforcement standards, participants used the occasion to create NOBLE.

The theme of the 2005 conference was "Living the Dream Through Justice by Action." The conference included an exhibit area with displays from numerous Federal agencies, local agencies, and private companies; a career fair; business meetings; speakers; and many informative and well-timed sessions. The training workshops included (1) Identity Theft, (2) Gang Awareness, (3) Internet Investigative Tools, (4) Rap Music and Its Influence on Youth, (5) Health Issues Affecting the Black Community, and (6) The Barriers of Race, Culture, and Faith.

The 29th Annual Training Conference and Exhibition was very well attended and received favorable comments from participants. The NRC OIG employees who attended found that the conference provided them with a great opportunity to exchange information with other law enforcement personnel and gain valuable insight into the issues facing law enforcement officers today.

NRC OIG Shares Expertise with Frederick County, Maryland

NRC OIG staff members George A. Mulley, Senior Level Assistant for Investigative Operations, and Cheryl Windsor, Investigative Analyst, met with two internal auditors from Frederick County, Maryland to share information on OIG's hotline program. The information provided was intended to assist the county in benchmarking its process for handling hotline complaints.

Topics covered included (1) sources of complaints, (2) classification codes for complaints, (3) forms used for complaints, (4) allegation tracking and hotline operations, (5) eliciting information from callers, (5) summarizing the complaints, and (6) developing a database to capture information. In addition to the topics discussed, the OIG staff provided some real life examples of hotline calls and how to respond to callers and capture the information.

The Frederick County internal auditors agreed that the information provided by NRC OIG was extremely valuable and would enable them to establish a quality hotline program.

OIG Staff Learn about France's Nuclear Program

In June 2005, OIG audit staff met with Regis P. Babinet, Counselor for Nuclear Energy, French Atomic Energy Commission, Embassy of France. The meeting was in support of OIG's audit to determine the effectiveness of NRC's oversight of byproduct materials. OIG staff contacted Dr. Babinet because the International Atomic Energy Agency and the U.S. Government Accountability Office recognized France's "best practices" in the tracking and control of nuclear materials. At the meeting with Dr. Babinet, OIG learned about France's organizational structure regarding its oversight of nuclear materials. Subsequent to the meeting, Dr. Babinet provided additional information requested by OIG audit staff. OIG found these contacts with Dr. Babinet to be very informative and appreciates the time and effort expended by the French Government.

Regis P. Babinet, Counselor for Nuclear Energy, French Atomic Energy Commission, Embassy of France (center) with members of the Office of the Inspector General staff pictured from left to right: Cheryl Miotla, Audit Manager; Hubert T. Bell, Inspector General; Dr. Babinet; Anthony Lipuma, Audit Team Leader; and Michael Cash, Engineering Technical Advisor.

In September 2005, OIG audit staff attended a meeting hosted by NRC with representatives from the French Directorate General of Nuclear Safety and Protection Against Radiation. The meeting agenda included discussions on risk-informing materials safety programs, tracking of sources, and status of import and export regulations.

To help the agency improve its effectiveness during this period, OIG completed 13 performance audits or evaluations that resulted in recommendations to NRC management. In two of its internal audits, OIG found $6,431,600 in funds that could be put to better use.

AUDIT SUMMARIES

Audit of NRC's Reactor Program System

OIG Strategic Goal: Corporate Management

The Nuclear Regulatory Commission's (NRC) mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. Fundamental to the regulatory process is NRC's commercial nuclear power plant inspection program, which assesses whether plant operations are properly conducted and equipment is properly maintained. Inspectors examine licensee activity, provide inspection findings to licensee managers, and conduct followup inspections to ensure that corrective actions are taken.

The Reactor Program System (RPS) is an information technology tool that provides planning, scheduling, and reporting capabilities to support the NRC reactor inspection and licensing programs. It is used by NRC managers to assess the effectiveness and uniformity of the implementation of those programs and related policies. The Office of Nuclear Reactor Regulation (NRR) and the regions use the RPS to schedule their work assignments and to plan and schedule licensing activities in NRR and inspection activities at nuclear power plants.

OIG conducted this audit to determine whether the RPS (1) provides for the availability, confidentiality, and integrity of the data stored in the system and (2) meets its required operational capabilities.

Audit Results. While the implementation of the RPS has allowed for a single system for entering inspection information, the information is not well protected, complete, or fully accurate. To ensure that the system meets operational requirements, NRC needs to:

- Comply with system access control requirements.
- Ensure accurate and timely inspection data.
- Improve management of the system help service.
- Improve the system configuration control process.
- Provide training to system users.

Without improvements to the RPS, NRC decisionmakers cannot rely on the information in the system or have a complete and accurate picture of the nuclear power plant inspection program. *(Addresses Management Challenges #2 and 5)*

Audit of NRC's Policy and Practices Concerning Camera Cell Phones

OIG Strategic Goal: Security

Camera cell phones, if misused, pose security and privacy threats because they enable people to covertly photograph images or scenes and transmit them immediately to the Internet. Approximately 20 percent of U.S. cell phone users had camera cell phones during 2004 and, according to analysts, by 2006, 80 percent of the cell phones sold in the U.S. will be camera phones.

Audit Results. NRC lacks a camera cell phone policy to:

- Establish requirements for the NRC acquisition of camera cell phone for use by employees.
- Remind employees and visitors that the prohibition against taking photographs in NRC buildings also applies to camera cell phones.
- Provide security guards with guidance on the handling of camera cell phones brought into the buildings by visitors.

Deliberate or careless use of camera cell phones can compromise classified or sensitive information or even physical security measures used to protect NRC facilities. The growing popularity of camera cell phones highlights the need to heighten employee and visitor awareness about NRC's prohibition against photographs inside agency facilities. *(Addresses Management Challenges #2 and 5)*

Audit of NRC's Telecommunications Program

OIG Strategic Goal: Security

NRC's telecommunications program includes local and long-distance voice services, voicemail, videoconferencing, and personal communications equipment (e.g., calling cards, cell phones). This audit focused primarily on the agency's non-secure telecommunications systems, although auditors also reviewed the agency's use of secure cell phones.

OIG conducted this audit to evaluate (1) controls over the use of NRC telecommunications services and (2) the physical security of NRC telecommunications systems.

Audit Results. 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.

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;

NRC is needlessly spending approximately $31,600 per year to pay for traveler's calls home; secure cell phones have failed to provide connectivity in several situations where users wanted secure calling capability; and agency telephone systems and other equipment maintained in equipment closets are vulnerable to tampering. *(Addresses Management Challenges #2 and 5)*

System Evaluation of Listed Systems That Process Safeguards and/or Classified Information

OIG Strategic Goal: Security

Listed systems that process safeguards and/or classified information require more security protections than the typical unclassified information processing systems. Many of the listed systems processing safeguards and/or classified information are either standalone personal computers or laptops. None of these systems are connected to the agency's local area network when processing safeguards and/or classified information. The objective of this system evaluation was to test the effectiveness or the security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information.

Audit Results. The evaluation determined that:

- The inventory of listed systems is inaccurate and information is inconsistent.
- Some listed systems lack required security plans.
- Some security controls are not implemented as required.

As a result, the agency cannot be certain that system sponsors/owners of listed systems processing safeguards and/or classified information have adequate controls in place to protect the information. *(Addresses Management Challenge #2)*

Review of NRC's Application of the Office of Management and Budget's Program Assessment Rating Tool (PART)

OIG Strategic Goal: Corporate Management

As part of the audit of NRC's Decommissioning Program, OIG examined aspects of the NRC's approach to applying PART. PART is a diagnostic tool intended to systematically and consistently assess the performance of program activities across the Federal Government. At the time of this report, five agency programs had been reviewed using PART and scored by the Office of Management and Budget (OMB). Four programs received an OMB rating of "Effective." One received a rating of "Moderately Effective."

Audit Results. While the agency's programs have scored well on PART reviews, OIG observed inconsistencies in the agency's approach. Specifically, NRC does not have agencywide guidance for applying PART to its programs to assure consistency in PART submittals and a common interpretation of OMB guidance. As a result, the value of PART to NRC as a tool for making continuous program improvements and informing management and budget decisions is diminished. *(Addresses Management Challenge #6)*

Audit of NRC's Contract Closeout Process

OIG Strategic Goal: Corporate Management

An expired contract is closed once it is both physically and administratively completed. The contract closeout process involves several administrative steps that can include, but are not limited to, settlement of subcontracts by the prime contractor; completion of a contract audit to determine final indirect and direct costs, if appropriate; payment of the final invoice; and deobligation of excess funds. The contract closeout process is subject to the requirements set forth in Federal Acquisition Regulation 4.804, "Closeout of contract files." The objectives of this audit were to determine whether:

- NRC's contract closeout policies and procedures adhere to applicable regulations.

- Management controls associated with the closeout process are adequate.
- NRC complies with its own closeout procedures, with an emphasis on timeliness.

Audit Results. The audit disclosed that NRC generally does not close expired contracts in accordance with Federal Acquisition Regulation required time standards. This delay is the result of inadequate policies and management's use of an incorrect performance metric. The audit also determined that there was approximately $6.4 million on 148 contracts awaiting closeout as of September 30, 2004, which had not been deobligated within 90 days of contract expiration, as required by NRC policy. The delay in deobligating these funds caused a delay in making the funds available for other agency priorities. *(Addresses Management Challenge #6)*

Audit of the Decommissioning Program

OIG Strategic Goal: Safety

Under the Government Performance and Results Act (GPRA) of 1993, Federal agencies are required to schedule, conduct, and report on program evaluations in selected areas. OMB developed the Program Assessment Rating Tool (PART) to assess and improve program performance so that the Federal Government can achieve better results and to help inform funding and management decisions. It builds on GPRA by encouraging agencies to integrate operational decisions with strategic and performance planning. NRC's FY 2006 performance plan identified NRC's decommissioning program as an activity scheduled to undergo a PART review and agency managers requested that OIG review this program.

NRC continues to regulate commercial nuclear reactors, fuel cycle facilities, and NRC material licensees after they are permanently shut down and begin decommissioning. Decommissioning is defined as removing a facility or site safely from service and reducing residual radioactivity to a level that permits (1) release of the property for unrestricted use and termination of the license or (2) release of the property under restricted conditions and termination of the license. In FY 2005, NRC conducted decommissioning licensing and inspection activities at 20 power reactors and at approximately 40 complex materials and fuel facilities sites.

The objective of this audit was to determine whether NRC's Decommissioning Program achieves the desired performance and results as stated in the agency's strategic plan, performance plan, and operating plan.

Audit Results. While NRC has processes in place to monitor, evaluate, and report on decommissioning program performance, OIG was unable to verify some performance results. In addition, NRC has not implemented changes as a result of an internal self-assessment that were intended to improve performance of the decommissioning program. *(Addresses Management Challenge #1)*

System Evaluation of Security Controls for Standalone Personal Computers and Laptops

OIG Strategic Goal: Security

NRC has an unknown number of standalone personal computers (PCs) or laptops, which require special security controls because they are not connected to the agency's local area network. The objective of this system evaluation was to evaluate the effectiveness of NRC security policies, procedures, practices, and controls for standalone PCs and laptops.

Audit Results. The evaluation determined that:

- Security controls for standalone PCs and laptops are not adequate.
- Standalone PCs and laptops are not monitored for compliance with Federal regulations.
- Information technology coordinators have inconsistent understanding of disposal practices for standalone PCs and laptops.

As a result, the agency cannot be certain that standalone PCs and laptops have adequate controls in place to protect the information processed on them. *(Addresses Management Challenge #2)*

Audit of NRC's Generic Communications Program

OIG Strategic Goal: Safety

NRC's primary means of communicating concerns or issues to licensees is through generic communications. These communications allow NRC to communicate and share industry experiences with applicable groups of licensees and other interested stakeholders. The information is relayed in writing to licensees in the form of Generic Letters, NRC Bulletins, Information Notices, and other documents. Some generic communications are intended solely to transmit information, while others request actions and require responses from licensee.

The purpose of this audit was to assess the effectiveness of the agency's generic communications program.

Audit Results. The audit identified generic communications, specifically safeguards advisories, that are issued outside of NRC's existing regulatory framework. As a result, the agency (1) may be unable to pursue actions requested or required of licensees in its generic communications and (2) compromises its openness policy, thereby affecting the public's confidence in NRC's regulatory processes and decisionmaking.

Additionally, controls for oversight of licensee action on generic communications are inadequate and NRC did not employ a sound methodology when conducting its effectiveness assessment of the Generic Communications Program. As a result, the agency risks the potential loss of safety/regulatory data and lacks assurance that its generic communications are effective. *(Addresses Management Challenges #1, 4, and 7)*

Evaluation of NRC's Certification and Accreditation Efforts

OIG Strategic Goal: Security

The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by the Federal Information Security Management Act (FISMA). Information systems under development must be certified and accredited prior to becoming operational. Operational information systems must be re-certified and re-accredited every 3 years in accordance with Federal policy, and whenever there is a significant change to the information

system or its operational environment. The objective of this audit was to evaluate the certification and accreditation efforts at NRC.

Results: 19 of 27 of operational NRC information systems are operating under an interim authorization to operate, and therefore are not considered certified and accredited. The information systems are not certified and accredited because:

- The certification and accreditation has lapsed or was never completed.
- NRC information systems are being re-certified and re-accredited using new requirements from the National Institute of Standards and Technology, which are proving difficult to meet.

(Addresses Management Challenge #2)

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2005

OIG Strategic Goal: Security

The Federal Information Security Management Act (FISMA) was enacted on December 17, 2002. FISMA outlines the information security management requirements for agencies, including the requirements for an annual review and annual independent assessment by agency Inspectors General. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The objective of the review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2005.

Results: NRC's information security program has several major weaknesses. Specifically:

- The majority of NRC systems have not been categorized in accordance with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- Agency self-assessments are not timely.
- Annual contingency plan testing is not being performed.

- Oversight of contractor systems is lacking.
- The agency's inventory of information systems is only 51-70 percent complete because (1) information in the two systems that maintain inventory information is inaccurate and inconsistent and (2) only one system contains information on system interfaces and that information is inaccurate and inconsistent. In addition, the agency's inventory is not maintained and updated annually.
- E-authentication risk assessments completed in accordance with OMB-04-04, *E-Authentication Guidance for Federal Agencies*, are incorrect and inconsistent with the systems' FIPS 199 security categorizations.
- Nineteen of the agency's 27 operational information systems are operating under an interim authorization to operate, and therefore are not considered certified and accredited.
- The agency lacks procedures for ensuring employees with significant information technology security responsibilities receive security training and awareness.

(Addresses Management Challenge #2)

Evaluation of NRC's Automated Information Inventory Process

OIG Strategic Goal: Security

FISMA outlines the information security management requirements for agencies, including the requirement to develop and maintain an inventory of major information systems operated by or under control of the agency. The agency maintains two inventories, the Information Technology Systems Security Tracking System and the Enterprise Architecture Repository System. The objective of this review was to evaluate NRC's process for maintaining an inventory of automated information systems.

Results: The evaluation found that:

- Information in NRC automated information system inventories is inaccurate and inconsistent.
- NRC automated information systems are not designed to capture all of the data needed to meet Federal requirements.

(Addresses Management Challenge #2)

Inspector General's Assessment of the Most Serious Management Challenges Facing NRC

OIG Strategic Goal: Corporate Management

On January 24, 2000, Congress enacted the Reports Consolidation Act of 2000 to provide financial and performance management information in a more meaningful and useful format for the Congress, the President, and the public. The act requires that the Inspector General of each Federal agency summarize what he or she considers to be the most serious management and performance challenges facing the agency and assess the agency's progress in addressing those challenges. The Inspector General, in his submission, defined serious management challenges as mission critical areas or programs that have the potential for a perennial weakness or vulnerability that, without substantial management attention, would seriously impact agency operations or strategic goals.

Audit Results. The Inspector General identified the following nine management challenges that are considered to be the most serious. The nine challenges are distinct but are interdependent. The NRC continues to address these challenges in its planning and day-to-day activities.

NRC's Most Serious Management Challenges as of September 30, 2005	
Challenge 1 Protection of nuclear material used for civilian purposes.	**Challenge 6** Administration of all aspects of financial management.
Challenge 2 Protection of information.	**Challenge 7** Communication with external stakeholders throughout NRC regulatory activities.
Challenge 3 Development and implementation of a risk–informed and performance–based regulatory approach.	**Challenge 8** Intra–agency communication (up, down, and across organizational lines).
Challenge 4 Ability to modify regulatory processes to meet a changing environment.	**Challenge 9** Managing human capital.
Challenge 5 Implementation of information resources.	The challenges are **not** ranked in any order of importance.

AUDITS IN PROGRESS

Audit of NRC's FY 2005 Financial Statements

OIG Strategic Goal: Corporate Management

Under the Chief Financial Officers Act and the Government Management and Reform Act, OIG is required to annually audit NRC's financial statements. OIG will audit NRC's financial statements in accordance with applicable auditing standards. The audit will express an opinion on the agency's financial statements, evaluate internal controls, review compliance with applicable laws and regulations, review the performance measures included in the financial statements for compliance with OMB guidance, and review the controls in the NRC's computer systems that are significant to the financial statements. In addition, OIG will be measuring the agency's improvements by assessing corrective action taken on prior years' audit findings. *(Addresses Management Challenge #6)*

Followup Audit of NRC's Decommissioning Fund Program

OIG Strategic Goal: Corporate Management

Under Title 10 Code of Federal Regulation (CFR) Part 50, NRC must receive reasonable assurances from nuclear reactor licensees that funds will be available for the decommissioning process. In the *Review of NRC's Decommissioning Fund Program,* issued in February 2000, OIG reported weaknesses in the management controls over NRC's decommissioning process. Among the weaknesses identified were lack of consistency in reported data and the need to determine the best method of assessing decommissioning costs at nuclear power plant sites. OIG reported that NRC's decommissioning formulas were developed in 1986 and could be outdated. The report noted that significant differences exist between two different methods used to calculate estimates for decommissioning costs. In response to OIG's findings, the Deputy Executive Director for Reactor Programs took no immediate action. Instead, implementation was delayed until a future time when more cost data would be available. Nineteen nuclear power plants have permanently shut down and are in some phase of decommissioning.

The objective of this audit is to evaluate NRC's actions on the FY 2000 OIG audit of NRC's decommissioning fund program. *(Addresses Management Challenge 6)*

Audit of the Office of Nuclear Security and Incident Response

OIG Strategic Goal: Security

In April 2002, NRC established the Office of Nuclear Security and Incident Response (NSIR) to consolidate and streamline selected NRC security, safeguards, and incident response responsibilities and resources. The office reports to the Deputy Executive Director for Homeland Protection and Preparedness. The formation of the office is one result of the Commission's ongoing top-to-bottom review of its safeguards and physical security program in the aftermath of the terrorist attacks of September 11, 2001.

Until NSIR was formed, the assessment of security responsibilities was determined by the type of facility requiring protection.

Until NSIR was formed, the assessment of security responsibilities was determined by the type of facility requiring protection. For example, the Office of Nuclear Material Safety and Safeguards was responsible for the security programs for protection of fuel cycle facilities, materials, transportation, disposal, and certain waste-storage facilities. The Office of Nuclear Reactor Regulation (NRR) was responsible for security programs at nuclear power plants and non-power reactors, decommissioning facilities, and certain spent fuel storage facilities. NRC determined that a centralized security organization would be a more effective and efficient way of organizing security activities.

NSIR has assumed responsibility for an important part of NRC's operations. As with any new organization, and especially one with such an important function, it must operate effectively and efficiently in order to meet its mission.

The objective of this audit is to conduct an independent evaluation of NSIR operations. *(Addresses Management Challenges #1, 2, 4, and 8)*

Audit of NRC's Oversight of Byproduct Materials and Sealed Sources

OIG Strategic Goal: Safety

Byproduct and sealed sources are used for medical, industrial, and academic purposes. Medical uses include medical procedures, medical research, and other diagnostic tests. Industrial uses of nuclear materials include industrial

radiography, irradiators, well-logging, gauging devices, other measuring systems, and research and development. Additionally, universities, colleges, high schools, and other academic institutions use byproduct and sealed source nuclear materials in classroom demonstrations, laboratory experiments, and research. NRC (or the responsible Agreement State) has regulatory authority over the possession and use of byproduct, source, or special nuclear material. In the post-September 11, 2001, environment, Congress continues to maintain interest in oversight of nuclear materials. An August 2004 letter to NRC from a member of Congress expressed concern regarding vulnerabilities that could be exploited by terrorists seeking to attack the United States.

The objective of this audit is to determine whether NRC's oversight of byproduct and sealed source materials provides reasonable assurance that licensees are using the materials safely and account for and control materials. *(Addresses Management Challenges #1 and 4)*

Audit of the Technical Training Center (TTC)

OIG Strategic Goal: Corporate Management

The NRC's Office of Human Resources manages training programs conducted at the TTC in Chattanooga, Tennessee. TTC, with a budget of $3.6 million and 27 FTE, conducts training programs related to the regulation of nuclear materials and facilities including nuclear power plant technology, radiation protection, risk assessment, and regulatory skills. Both Agreement State students and agency employees attend TTC courses.

The objective of this audit will be to identify opportunities to improve the economy, efficiency, and/or effectiveness of TTC's operations in consonance with the President's Management Agenda. *(Addresses Management Challenge #9)*

Safety Culture and Climate Survey

OIG Strategic Goal: Corporate Management

In 2002, OIG engaged an independent contractor to (1) assist in completing an assessment of the agency's safety culture and climate, (2) compare the results against NRC's 1998 Safety Culture and Climate Survey, and (3) compare the results to Government and national benchmarks.

The 2002 survey showed that NRC had made substantial progress in improving its safety culture and climate since the 1998 survey. The survey identified areas for improvement and recommended that NRC senior management focus on improvement in these areas. In response to the results of the survey, the Chairman tasked the Executive Director for Operations (EDO) to conduct an assessment of the key areas for improvement and establish priorities for NRC attention. With Commission approval, the EDO established a task group to evaluate the key areas identified in the OIG's report and to develop recommendations for improvement strategies. On July 25, 2003, the task group issued its report containing a recommendation that the agency focus its improvement efforts on four major areas.

The objective of this survey will be to: (1) assess the agency's safety culture and climate, (2) compare the results against NRC's 1998 and 2002 Safety Culture and Climate Surveys, and (3) compare the results to Government and national benchmarks. *(Addresses Management Challenge #8)*

Integrated Personnel Security System

OIG Strategic Goal: Corporate Management

The Division of Facilities and Security, Office of Administration, plans, develops, establishes, and administers policies, standards, regulations, and procedures for the overall NRC security program. The personnel security program is a significant part of the overall security program and strategy. The Atomic Energy Act of 1954 requires that all NRC employees have a security clearance. NRC's personnel security program retains personnel security and database files on more than 15,000 persons (active and retired). NRC sought to develop, deploy, and support an efficient, accurate system to replace its automated personnel security system. The replacement system, the Integrated Personnel Security System, was intended to provide NRC with an integrated system that meets the specified capabilities through the use of a Web-enabled system that allows authorized users access through the NRC Intranet.

The objectives of this audit will be to determine if the system meets its required operational capabilities. *(Addresses Management Challenges #2 and 5)*

INVESTIGATIONS

During this reporting period, the OIG received 108 allegations, initiated 38 investigations and 2 Event Inquiries, and closed 51 cases and 2 Event Inquiries. In addition, 13 cases were referred to the Department of Justice and 19 were forwarded to NRC management.

INVESTIGATIVE CASE SUMMARIES

Special Inquiry: NRC's Oversight of the Hope Creek Nuclear Generating Station

OIG Strategic Goal: Safety

Hope Creek Nuclear Generating Station

OIG conducted an investigation based on information that Region I, NRC, should have been aware of underlying equipment and operational problems at the Hope Creek Nuclear Generating Station that surfaced after an October 2004 drain tank pipe failure. The allegation further indicated that the underlying plant problems caused Hope Creek plant operators to voice strong reservations to Hope Creek management about the planned restart of the plant following repair of the drain tank pipe.

In addition to the Hope Creek restart issue, OIG received allegations involving lack of regulatory oversight by the NRC staff in the following areas:

- The Hope Creek and Salem Creek Nuclear Generating Stations Safety Conscious Work Environment.
- January 2005 management changes at Hope Creek which did not follow the Public Service Enterprise Group's (PSEG) Executive Review Board (ERB) process.
- Technical system problems including the Hope Creek's "B" recirculation pump, Reactor Core Isolation Cooling System, and High Pressure Coolant Injection System.
- Failure to properly address allegations of discrimination by PSEG management.

OIG determined that following repair of the drain tank pipe, appropriate discussions occurred between Hope Creek management and plant operators which resulted in the decision by management to keep the plant offline and to transition into a scheduled refueling outage. A special NRC inspection team reviewed circumstances surrounding the October 2004 drain tank pipe failure and concluded that PSEG's overall response was adequate and that none of the problems would have prevented the systems from performing their intended safety functions.

OIG learned that the NRC Region I allegations staff substantiated the alleger's concern that the work environment at the Salem and Hope Creek stations needed improvement. The NRC plans to monitor PSEG's efforts to improve the work environment at these stations. Region I reviewed and confirmed the allegation that the ERB process was not used to assess the January 2005 management changes at Hope Creek. Region I requested that PSEG reassess the ERB issue to determine if it was being fully implemented. Also, Region I advised the alleger that it was monitoring the ERB issue and will continue providing heightened regulatory oversight of this issue until progress has been confirmed.

With respect to the alleger's numerous technical concerns regarding systems or programs at Hope Creek, OIG found that Region I reviewed each concern and kept the alleger informed as to the status of concerns raised in accordance with the NRC Management Directives.

OIG found that the allegations staff and Office of Investigations, Region I, NRC, appropriately handled the alleger's discrimination claim consistent with the NRC Management Directives. *(Addresses Management Challenges #1 and 3)*

Adequacy of NRC's Oversight of Vermont Yankee Power Uprate Review Process

OIG Strategic Goal: Safety

In response to a Congressional request and allegations from the public, OIG conducted an Event Inquiry to determine the adequacy of NRC's oversight of the Vermont Yankee Nuclear Power Station (VYNPS) extended power uprate (EPU) review process. OIG addressed allegations as to whether NRC was following

its process, if the NRC staff was being pressured by or colluding with General Electric (GE) and/or Entergy, and if the NRC staff made misleading statements to the public pertaining to the VYNPS EPU.

Following the licensee's proposed license amendment request to increase its maximum authorized power level, termed an extended power uprate, members of the public questioned NRC's allowing the licensee, in calculating the available net positive suction head (NPSH) of safety-related pumps, to take credit for a large amount of containment accident pressure over a long period of time. According to the public, this was inconsistent with the NRC's Regulatory Guide (RG) 1.82, Rev. 3, (Water Sources for Long Term Re-circulation Cooling Following a Loss-of Coolant Accident), dated November 2003 and the NRR Standard Review Plan 001, published in December 2003. The NRC guidance documents state that credit for containment accident pressure in calculating the available NPSH of safety-related pumps should be minimized to the fullest extent possible. The public stated that, in recent years, NRC has approved some licensee amendment requests for EPUs that took credit for a small amount of containment accident pressure over a short period of time. However, the public noted that this was not the case in VYNPS's EPU request; consequently, the public stated that NRC was not following its process in this review.

OIG found that since 2001, the NRC has consistently interpreted and applied its interpretation of RG 1.82 in approving five other EPUs. However, the NRC acknowledged that the language in RG 1.82 was not clear and began work to revise RG 1.82 to more accurately reflect the agency's position that credit can be taken for containment accident pressure. NRC will also revise the NRR Standard Review Plan 001 to make it consistent with the RG 1.82.

OIG did not find evidence of NRC staff colluding or bowing to pressure from GE or Entergy, and did not substantiate allegations pertaining to misleading statements being made to the public. OIG also received three allegations relating to the NRC staff being pressured by or colluding with GE and/or Entergy during the Vermont Yankee power uprate review process and four allegations that NRC staff provided misleading and/or inaccurate statements to the public regarding the Vermont Yankee EPU. *(Addresses Management Challenges #1 and 3)*

False Claims of Small Business Status by NRC Licensee

OIG Strategic Goal: Corporate Management

OIG conducted an investigation of a materials licensee in Puerto Rico and its president as a result of a review of the NRC Small Business Entity Status Program. Title 10 Code of Federal Regulations (CFR) Part 171 provides that a materials licensee who qualifies as a small business entity may be eligible for a reduced annual NRC licensee fee. The criteria NRC uses to determine whether a business qualifies as a small business entity eligible for a reduced fee are based upon specific size standards. One of these standards is the amount of the applicant's gross receipts for a period of time. OIG learned that the materials licensee in Puerto Rico submitted five NRC Forms 526, *Certification of Small Entity Status for the Purposes of Annual Fees Imposed under 10 CFR Part 171*, for FYs 2001 through 2005. To receive a reduced annual license fee, the licensee claimed on each form that its gross receipts were less than $350,000.

OIG determined that for fiscal years (FYs) 2001 through 2005, the owner signed and submitted five NRC Forms 526, falsely certifying to the NRC that the company was a small business entity. OIG determined that the owner significantly under-reported the company's gross receipts to the NRC by claiming that its gross receipts averaged less than $350,000 a year. As a result of falsely claiming a small business status, the licensee benefitted from reduced annual licensee fees for the NRC license for 5 fiscal years and underpaid the NRC a total of $55,500. *(Addresses Management Challenge #6)*

Adequacy of NRC Oversight of Lost Nuclear Material

OIG Strategic Goal: Safety

OIG conducted an investigation into NRC's handling of a report that two radioactive sources imported from Russia by a private firm were missing. The sources were reported missing several months after clearing Customs on October 9, 2004, in New York. On February 8, 2005, the firm reported to NRC

that the sources never arrived at the company's facility and could not be located. NRC reported the incident to the Federal Bureau of Investigation which subsequently found the missing sources on February 9, 2005, at a shipping facility in Boston, Massachusetts.

As a result of the investigation, OIG determined that NRC staff first learned of the missing sources on February 8, 2005, after the company contacted the NRC to report the missing sources. On the same day, NRC Region I notified New York and New Jersey State officials of the incident. On March 15, 2005, NRC Region IV conducted an inspection of the firm's facility in Houston, Texas, and State of Texas officials also conducted an inspection of the firm. Neither the State of Texas nor Region IV identified any violations. NRC staff found that (1) a contractor was responsible for shipping the sources for the firm and the contractor did not report the sources missing to the firm until February 7, 2005, and (2) the weight of the individual two sources did not meet the reporting requirement threshold that required the licensee to notify NRC within 24-hours of learning that radioactive sources were missing. Region I conducted a "lessons-learned evaluation" of the incident for its failure to notify Massachusetts officials that the missing sources were found in their State. Region I acknowledged that although there was no written requirement to do so, they should have informed Massachusetts officials. *(Addresses Management Challenge #1)*

Unauthorized Practice of Law by NRC Attorney

OIG Strategic Goal: Corporate Management

OIG conducted an investigation following information that an NRC attorney entered Notices of Appearance and represented NRC staff in NRC administrative court proceedings before the Atomic Safety and Licensing Board Panel (ASLBP) and practiced law without the required active attorney bar membership.

OIG found that between September 2003 and June 2004, the attorney submitted two Notices of Appearance before the ASLBP in which he falsely attested that he was admitted to practice law before the State of Maryland. As a result, he was permitted to practice law before the ASLBP. OIG determined that between April 8, 2003, and April 14, 2005, the attorney was not authorized to practice law due to his inactive status with the Client Protection Fund of the Bar of Maryland

(Bar of Maryland). The employee resigned from his position at the NRC. *(Addresses Management Challenge #9)*

False Academic Credentials Provided by NRC Employee

OIG Strategic Goal: Corporate Management

During an OIG initiative to review academic credentials of NRC employees, OIG discovered that an NRC employee had listed a fictitious Bachelor of Science degree on a Standard Form 86, Questionnaire for National Security Positions, and entered this information into the NRCareers Federal Online Job Application System which was submitted for a promotion at NRC. The employee also listed a fictitious Associate of Arts degree and a business-related certificate on five previous NRC employment applications submitted through the NRCareers Federal Online Job Application System.

OIG found that the employee's Bachelor of Science degree was from an Internet-based diploma mill which was not accredited by the Department of Education and was categorized by two States as a school whose degrees did not meet educational requirements for State employment or professional licensing. OIG also determined that the employee did not earn the business certificate as claimed. As a result of the OIG investigation, the employee resigned from the NRC. *(Addresses Management Challenges #2 and 9)*

Allegation of Fraud by NRC Vendor

OIG Strategic Goal: Corporate Management

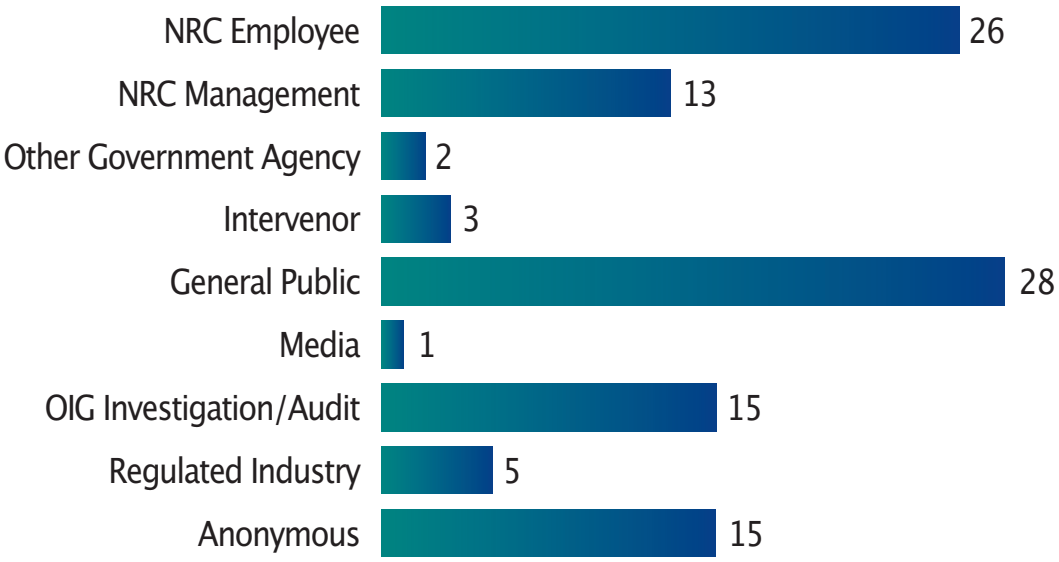
OIG conducted an investigation based on information that a Federal Government vendor was suspected of double billing, fraudulently adding freight/shipping charges to purchases, and selling non-trade compliant equipment to the Federal Government. The alleger reported that the fraud against the Government pertained to Blanket Purchase Agreement (BPA) contracts where the vendor double billed agencies for equipment, added freight/shipping charges to invoices which were not authorized in the BPA, and sold non-trade compliant equipment.

OIG determined that the NRC had a total of 11 Orders for Supplies and Services in the amount of $162,800 to purchase equipment from the vendor. After reviewing all orders and comparing them to Federal Financial System data on payments made by NRC to the vendor, OIG found that NRC was billed only for requested equipment and received all equipment ordered. OIG found no indication of double billing or purchases of non-trade compliant equipment. *(Addresses Management Challenge #6)*

STATISTICAL SUMMARY OF OIG ACCOMPLISHMENTS

INVESTIGATIVE STATISTICS

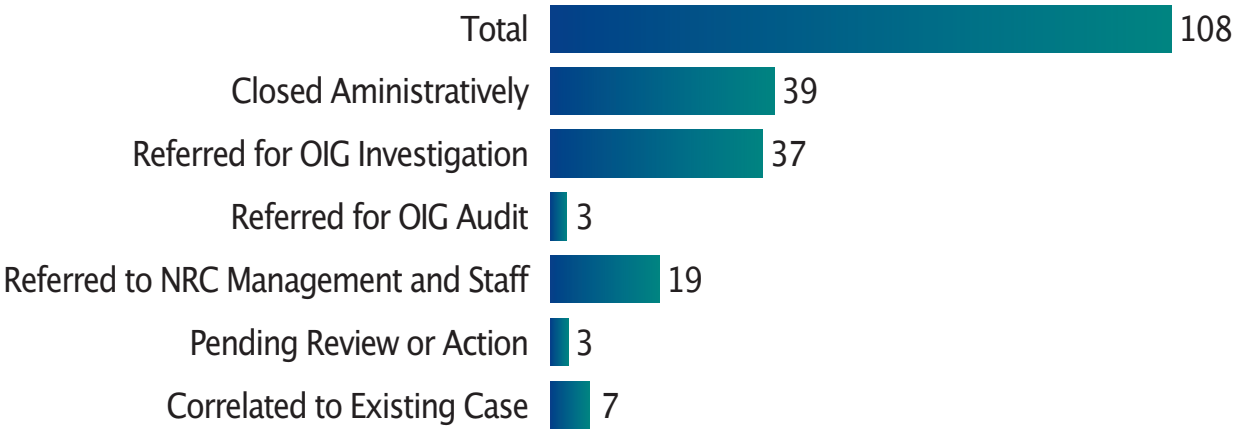
Source of Allegations — April 1, 2005, through September 30, 2005



Allegations resulting from Hotline calls: 17

Total: 108

Disposition of Allegations — April 1, 2005, through September 30, 2005



STATUS OF INVESTIGATIONS

DOJ Referrals 13
State Referrals 1
State Declinations 1
DOJ Declinations 12
DOJ Acceptance 1
Indictments and Arrests 1
Convictions 1
Sentencing 1
PFCRA Referral 1

NRC Administrative Actions:
- Terminations and Resignations 7
- Suspensions and Demotions 2
- Counseling 3
- Letter of Reprimand 2
- Other Administrative Action 2

SUMMARY OF INVESTIGATIONS

Classification of Investigations	*Carryover*	*Opened Cases*	*Closed Cases*	*Cases In Progress*
Conflict of Interest	2	0	1	1
Internal Fraud	0	1	0	1
External Fraud	7	3	7	3
False Statements	1	0	1	0
Theft	0	0	0	0
Misuse of Government Property	9	5	11	3
Employee Misconduct	2	11	11	2
Management Misconduct	1	4	4	1
Technical Allegations — Other	7	11	13	5
Proactive Initiatives	0	3	3	0
Total Investigations	**29**	**38**	**51**	**16**
Event Inquiries	4	2	2	4

AUDIT LISTINGS

Internal Program Audit and Special Evaluation Reports

Date	*Title*	*Audit Number*
4/13/05	Audit of NRC's Reactor Program System	OIG-05-A-11
6/7/05	Audit of NRC's Policy and Practices Concerning Camera Cell Phones	OIG-05-A-12
6/7/05	Audit of NRC's Telecommunications Program	OIG-05-A-13
8/4/05	System Evaluation of Listed Systems that Process Safeguards and/or Classified Information	OIG-05-A-14
8/26/05	Review of NRC's Application of the Office of Management and Budget's Program Assessment Rating Tool (PART)	OIG-05-A-15
8/26/05	Audit of NRC's Contract Closeout Process	OIG-05-A-16
9/21/05	Audit the Decommissioning Program	OIG-05-A-17
9/22/05	System Evaluation of Security Controls for Standalone Personal Computers and Laptops	OIG-05-A-18
9/30/05	Audit of NRC's Generic Communications Program	OIG-05-A-19
9/30/05	Evaluation of NRC's Certification and Accreditation Efforts	OIG-05-A-20
9/30/05	Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2005	OIG-05-A-21
9/30/05	Evaluation of NRC's Automated Information System Inventory Process	OIG-05-A-22
9/30/05	Inspector General's Assessment of the Most Serious Management Challenges Facing NRC	OIG-05-A-23

Contract Audit Reports

OIG Issue Date	*Contractor/ Contract Number*	*Questioned Costs*	*Unsupported Costs*
04/14/05	Southwest Research Institute		
	NRC-02-01-005	$2,412	0
	NRC-02-03-002	0	0
	NRC-02-03-004	0	0
	NRC-02-03-005	0	0
	NRC-02-03-007	0	0

AUDIT RESOLUTION ACTIVITIES

TABLE I

OIG Reports Containing Questioned Costs[1]
April 1, 2005 – September 30, 2005

Reports	*Number of Reports*	*Questioned Costs (Dollars)*	*Unsupported Costs (Dollars)*
A. For which no management decision had been made by the commencement of the reporting period	2	$43,547	$3,606,365[2]
B. Which were issued during the reporting period	1	$2,412	0
Subtotal (A + B)	3	$45,959	$3,606,365
C. For which a management decision was made during the reporting period:			
(i) dollar value of disallowed costs	1	$2,412	0
(ii) dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	2	$43,547	$3,606,365
E. For which no management decision was made within 6 months of issuance	2	$43,547	$3,606,365

[1]Questioned costs are costs that are questioned by the OIG because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; a finding that, at the time of the audit, such costs are not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

[2]The General Services Administration (GSA) is responsible for the management decision on these questioned and unsupported costs. GSA has advised that the decision will be made sometime in early 2006.

TABLE II

OIG Reports Issued with Recommendations That Funds Be Put to Better Use[3] April 1, 2005 – September 30, 2005

Reports	*Number of Reports*	*Dollar Value of Funds*
A. For which no management decision had been made by the commencement of the reporting period	0	0
B. Which were issued during the reporting period	2	$6,431,600[4]
C. For which a management decision was made during the reporting period:		
(i) dollar value of recommendations that were agreed to by management	2	$6,431,600[4]
(ii) dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision had been made by the end of the reporting period	0	0
E. For which no management decision was made within 6 months of issuance	0	0

[3]A "recommendation that funds be put to better use" is a recommendation by the OIG that funds could be used more efficiently if NRC management took actions to implement and complete the recommendation, including: reductions in outlays; deobligation of funds from programs or operations; withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; costs not incurred by implementing recommended improvements related to the operations of NRC, a contractor, or a grantee; avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or any other savings which are specifically identified.

[4]See audit report summaries on pages 13, 14, 15 and 16.

TABLE III

Recommendations Described in Previous Semiannual Reports on Which Corrective Action Has Not Been Completed

Date	*Report Title*	*Number*
05/26/03	Audit of NRC's Regulatory Oversight of Special Nuclear Materials	OIG-03-A-15
	Recommendation 1: Conduct periodic inspections to verify that material licensees comply with MC&A (material control and accountability) requirements, including, but not limited to visual inspections of licensees' SNM (special nuclear material) inventories and validation of reported information.	
	Recommendation 5: Establish an independent NRC system of accounting for SNM possessed by NRC and Agreement State licensees and ensure that beginning balances are accurate based on NRC's physical verification of a statistical sample of the location and amounts of SNM held by licensees or a review of a statistical sample of a licensee's records or some combination thereof.	
05/24/04	Review of NRC's Drug-Free Workplace Plan	OIG-04-A-15
	Recommendation 3: Obtain U.S. Department of Health and Human Services approval of the *NRC Drug-Free Workplace Plan* prior to implementation.	
09/16/04	Audit of NRC's Incident Response Program	OIG-04-A-20
	Recommendation 1: Establish a defined agency-wide incident response plan that includes standards for performance, delineation of the conduct of exercises and drills, and a well-defined objective mechanism for evaluating incident response during exercises.	

TABLE III *(continued)*

Recommendations Described in Previous Semiannual Reports on Which Corrective Action Has Not Been Completed

Date	*Report Title*	*Number*
11/12/04	Results of the Audit of the U.S. Nuclear Regulatory Commission's Financial Statement for the Fiscal Years 2004 and 2003	OIG-05-A-02

Recommendation 1: The CFO (Chief Financial Officer) should ensure that the functionality of interfaces is rigorously tested before placing any software changes into production. Acceptance testing scripts should be designed more broadly to ensure greater scrutiny of the change being implemented. Independent validations of software changes and the related acceptance testing should be performed or reviewed and approved by persons other than those requesting the software modifications.

Recommendation 2: The CFO should develop and implement a remediation plan to enhance the reliability of the current billing system. Additionally, as the CFO considers the system redesign they should identify steps to address systemic issues with the current fee billing system.

Recommendation 3: The CFO should ensure that documented, complete and reliable quality assurance procedures are prepared for the billing process. At a minimum, those procedures should provide for a documented global reconciliation, at each billing cycle, of hours and fees reflected in FEES to the invoices generated by the PC-based fee billing systems.

ABBREVIATIONS AND ACRONYMS

ASLBP	Atomic Safety Licensing Board Panel
BPA	Blanket Purchase Agreement
CFR	Code of Federal Regulations
DAEO	Designated Agency Ethics Official
DOE	U.S. Department of Energy
EDO	Executive Director for Operations (NRC)
ERB	Executive Review Board
EPU	extended power uprate
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GE	General Electric
GPRA	Government Performance and Results Act
IAM	Issue Area Monitor
IG	Inspector General
IT	information technology
MD	Management Directive
MIS	management information system
NOBLE	National Organization of Black Law Enforcement Executives
NPSH	net positive suction head
NRC	U.S. Nuclear Regulatory Commission

NRR	Office of Nuclear Reactor Regulation (NRC)
NSIR	Office of Nuclear Security and Incident Response (NRC)
NWPA	Nuclear Waste Policy Act
OGE	U.S. Office of Government Ethics
OIG	Office of the Inspector General (NRC)
OMB	U.S. Office of Management and Budget
PART	Program Assessment Rating Tool
PBPM	Planning, Budget, and Performance Management
PC	personal computer
PSEG	Public Service Enterprise Group
RIF	Reduction in Force
RG	Regulatory Guide
RPS	Reactor Program System
SES	Senior Executive Service
SISP	Sensitive Information Screening Project
TTC	Technical Training Center (NRC)
VYNPS	Vermont Yankee Nuclear Power Station

REPORTING REQUIREMENTS

The Inspector General Act of 1978, as amended (1988), specifies reporting requirements for semiannual reports. This index cross-references those requirements to the applicable pages where they are fulfilled in this report.

CITATION	REPORTING REQUIREMENTS	PAGE
Section 4(a)(2)	Review of Legislation and Regulations	4
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	11-21, 26-32
Section 5(a)(2)	Recommendations for Corrective Action	11-21
Section 5(a)(3)	Prior Significant Recommendations Not Yet Completed	39-40
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	34
Section 5(a)(5)	Information or Assistance Refused	None
Section 5(a)(6)	Listing of Audit Reports	35
Section 5(a)(7)	Summary of Significant Reports	11-21, 26-32
Section 5(a)(8)	Audit Reports — Questioned Costs	37
Section 5(a)(9)	Audit Reports — Funds Put to Better Use	38
Section 5(a)(10)	Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made	37
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions With Which OIG Disagreed	None

NRC OIG'S STRATEGIC GOALS

1. Advance NRC's efforts to enhance safety and protect the environment.

2. Enhance NRC's efforts to increase security in response to the current threat environment.

3. Improve the economy, efficiency, and effectiveness of NRC corporate management.

The NRC OIG Hotline

The Hotline Program provides NRC employees, other Government employees, licensee/utility employees, contractors and the public with a confidential means of reporting suspicious activity to the OIG. We do not attempt to identify persons contacting the Hotline.

What should be reported:

- Contract and Procurement Irregularities
- Conflicts of Interest
- Theft and Misuse of Property
- Travel Fraud
- Misconduct
- Abuse of Authority
- Misuse of Government Credit Card
- Time and Attendance Abuse
- Misuse of Information Technology Resources
- Program Mismanagement

Ways to Contact the OIG

Call:
OIG Hotline
1-800-233-3497
TDD: 1-800-270-2787
7:00 a.m. – 4:00 p.m. (EST)
After hours, please leave a message

Submit:
On-Line Form
www.nrc.gov
Click on Inspector General
Click on OIG Hotline

Write:
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program, MS T5 D28
11545 Rockville Pike
Rockville, MD 20852-2738

NUREG-1415, VOL. 18, NO. 1