



# *Office of the Inspector General*

---

*U.S. Nuclear Regulatory Commission*



---

*Semiannual Report*

*April 1, 2003 – September 30, 2003*



## THE SEAL AND BADGES OF THE NUCLEAR REGULATORY COMMISSION OFFICE OF THE INSPECTOR GENERAL

Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) audit and investigative personnel carry credentials issued by the Inspector General and marked with a distinct seal or badge, respectively, that identifies the bearer's NRC/OIG affiliation and defines their authority and responsibilities.

In its early years, staff of OIG's predecessor, the Office of Inspector and Auditor carried credentials but no badges.

Upon creation of the OIG in April 1989, Inspector General, David C. Williams, authorized Special Agents to carry a gold-plated badge. This badge, shown above left, was issued in 1990 and used until 1996 and featured the Special Agent and Inspector General titles surrounding the NRC seal.

Following the appointment of Inspector General Hubert T. Bell in July 1996, the gold badge gave way to a similar badge accented in blue. The blue and gold badge, depicted above center, enhanced the wording for identification purposes and was used by Special Agents from 1997 to 2003.

In 2003, a new badge was designed after the events of September 11, 2001. The new badge, displayed on the right above, features a sunburst rising from the NRC seal and incorporates our national colors.

Also, in 2003, the NRC OIG created an official office seal, shown below. This seal incorporates our national colors and depicts the American eagle holding an olive branch and arrows with a flag insignia. This new seal is used by the audit staff on their credentials.



---

# MEMORANDUM TO THE CHAIRMAN

On behalf of the Office of the Inspector General (OIG) for the U.S. Nuclear Regulatory Commission (NRC), I am pleased to submit this *Semiannual Report* to the U.S. Congress. This report summarizes significant OIG activities during the period from April 1, 2003, to September 30, 2003, in compliance with Sections 4 and 5 of the Inspector General (IG) Act of 1978, as amended.

During this reporting period, our office completed 10 performance and financial audits of NRC's programs and operations. This work led OIG to make a number of recommendations and suggestions to the NRC for program improvement. In addition, OIG completed 52 investigations, 2 Event Inquiries, 1 special project and made 31 referrals to NRC management. These investigations resulted in \$73,527 in recoveries and \$421,000 in cost savings to the Federal Government. Finally, OIG analyzed eight contract audit reports, two of which identified \$205,396 in questioned costs. NRC has disallowed the entire \$205,396.

This year is especially significant in that it marks the 25<sup>th</sup> anniversary of the enactment of the IG Act of 1978. In celebrating the many accomplishments of the IG community, NRC OIG will use this next year as an opportunity to reflect, both individually and as a community, on the successes of our past and how we can continue to build on our accomplishments. In the next year, the IG community is looking to engage the Administration and the Congress in a dialogue on ways to improve upon the IG Act. The IGs as a community hope to share our past and articulate our vision for the future.

Finally, I would like to express my appreciation to Congress, as well as NRC's senior management, for their support of OIG's mission. We are committed to working together to carry out the mission established for us 25 years ago. We also look forward to working with the Administration, Congress, the Commission, and NRC staff in addressing the current and future challenges facing our Government.

Sincerely,



Hubert T. Bell

---



---

# CONTENTS

<b>Executive Summary</b> .....	v
<b>The Office of the Inspector General</b> .....	1
History of the Inspector General Act .....	1
Organization and Functions of NRC's OIG .....	2
<b>The Nuclear Regulatory Commission — Regulator of Nuclear Safety</b> .....	5
Why NRC Regulates .....	5
How NRC Regulates .....	6
Management Challenges Facing NRC Identified by OIG .....	7
<b>The Audit Program</b> .....	9
Audit Summaries .....	9
Audits in Progress .....	13
<b>The Investigative Program</b> .....	17
Investigative Case Summaries .....	17
Investigative Statistics .....	21
<b>Other Activities</b> .....	23
Regulatory Review .....	23
The IG at the NRC .....	24
Training at the Inspectors General Institute .....	25
NRC OIG Tactical Training Facility .....	25
<b>Appendices</b> .....	27
Audit Listings .....	27
Audit Tables .....	29
Abbreviations .....	31
Reporting Requirements Index .....	32



---

# EXECUTIVE SUMMARY

*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

- OIG conducted a computer security review at NRC's regional offices located in King of Prussia, Pennsylvania (Region I); Atlanta, Georgia (Region II); Lisle, Illinois (Region III); and Arlington, Texas (Region IV).

The security reviews found that the controls implemented by the regions are generally effective in reducing the risks associated with their operations. However, several areas need improvement. These areas include administrative security controls, information technology controls, physical security controls, safety controls, and supporting utilities. Because the reports contain sensitive unclassified information, the details of the areas needing improvement are not available for public dissemination.

- NRC is authorized to grant licenses for the possession and use of special nuclear material (SNM) and establish regulations to govern the possession and use of such material. Practical uses of SNM include (1) fuel for nuclear reactors; (2) industrial, academic, and medical research and testing; and (3) the manufacture of industrial gauging devices (sealed sources). NRC's Commission states that proper control and accounting of SNM is an important component of the agency's safeguards and security programs.

Today's heightened sensitivity to the control of SNM warrants NRC's serious attention to

its licensees' material control and accounting activities. However, NRC's current levels of oversight of licensee Material Control and Accountability (MC&A) activities do not provide adequate assurance that all licensees properly control and account for SNM. Specifically, NRC performs limited inspections of licensee MC&A activities and cannot assure the reliability of the federally established and managed SNM tracking system.

Without adequate inspections to verify licensees' commitments to MC&A, or a reliable SNM tracking system, NRC has no independent means for determining if SNM was lost, stolen, or otherwise diverted while in a licensee's possession. Despite not being a regulatory requirement, having this independent ability would enhance the agency's oversight abilities.

- OIG conducted an audit of NRC's oversight of research and test reactors. Research and test reactors (also called non-power reactors) are nuclear reactors whose primary function is the safe conduct of research and development activities. Almost every field of science makes use of these reactors, which are also used to educate students for careers in the nuclear power industry, national defense, and research. The NRC currently licenses 50 research and test reactors. Thirty-five of those are operating

*(continued on next page)*

in 23 States. Fifteen others are no longer operating and are being decommissioned.

Oversight of research and test reactors was meeting NRC's expectations. Staff met goals for reviewing and approving licensee requests for changes to their licenses and licensee demand to license reactor operators. In addition, inspection requirements were generally satisfied.

However, some aspects of oversight can be improved. Specifically, NRC can (1) improve guidance for inspection followup items to describe for *licensees* what an inspection followup item means in regulatory terms, (2) improve operating plans to represent a discrete level of activity so that management can monitor performance and resource usage, (3) increase the availability of information so that the public can effectively participate in or make reasonable judgments about the adequacy of NRC's research and test reactor inspection program, and (4) document inspector training so that employee training records show compliance with training requirements.

- **OIG audited the NRC's information security program in accordance with the requirements of the Federal Information Security Management Act (FISMA). The objectives of the evaluation were to (1) test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assess compliance with the FISMA and related information security policies, procedures, standards, and guidelines.**

Over the past year, NRC has improved its security program and is implementing corrective actions from the 2002 Government Information Security Reform Act

review. However, several areas need improvement. First, the NRC Operating and System Software Maintenance Procedures are not followed consistently, contributing to an incomplete inventory of NRC operating and system software. Second, new weaknesses and corrective actions identified during the past fiscal year were not always added to the system that tracks corrective actions. Third, recent computer security reviews of the four NRC regional offices found systems on NRC's master inventory that either do not meet the criteria for inclusion on the list or are no longer being used. The inventory is currently being reviewed and updated to ensure that only those systems that meet the criteria defined in Management Directive (MD) 12.5 are included.

## **INVESTIGATIONS**

- **OIG completed an Event Inquiry into NRC's regulatory oversight of the operations at the Oconee and North Anna Nuclear Power Stations relating to leakage from reactor pressure vessel (RPV) heads. OIG received allegations that between Spring 2001 and Spring 2003, NRC allowed Oconee Units 1, 2, and 3 and North Anna Unit 1 to operate with known or suspected RPV head leakage in violation of plant technical specifications and that NRC took no enforcement action against the licensees for those violations. As a result of this inquiry, OIG found no evidence that the NRC staff permitted the licensees of Oconee or North Anna power plants to operate with known or suspected leakage of the RPV head. Specifically, OIG learned that the licensees for Oconee and North Anna utilized acceptable techniques during outages to inspect for cracking and leakage. In each case where leakage was**



---

discovered, NRC staff reviewed licensees' repairs and determined that the repairs were appropriately implemented. Additional RPV head leakage found during subsequent outages was also repaired before restarting the plants. OIG also learned that because of the potential for continuing RPV head leakage, both units at North Anna replaced their vessel heads. Oconee Unit 3 also recently completed the replacement of its vessel head, and Units 1 and 2 are scheduled for vessel head replacement in Fall 2003 and Spring 2004, respectively.

- OIG completed an investigation pertaining to a former NRC employee who was provided a Discontinued Service Retirement (DSR) to which he was not entitled. OIG received information that the employee, who was under consideration for termination as a result of misconduct, received a DSR from NRC after declining to be reassigned outside of his commuting area. This investigation disclosed that the NRC entered into a settlement agreement with the employee which improperly provided the employee a DSR. This investigation resulted in a \$61,457 recovery and \$421,000 in cost savings to the Federal Government.
- OIG completed a proactive review for fiscal years 2001 through 2003 to identify the potential misuse of information technology resources by NRC employees and contractors. OIG completed 30 investigations of NRC employees and contractors who misused their Government computers.

As a result of the investigations, OIG found that 22 NRC employees and 7 contractor employees accessed Internet sites containing sexually explicit material on their assigned NRC computer. Additionally, OIG discovered that employees of the NRC contract guard force were utilizing NRC

issued computers to access sexually explicit material.

Responsive action taken by the NRC as to its employees ranged from a 21-day suspension to job termination. NRC negotiated with the contractor for the guard force and a contractor providing computer services to deduct more than \$17,000 in NRC payments made to the contractors for hours spent by the contractors engaging in these unapproved and non-contract related activities.

- OIG completed an Event Inquiry into NRC's oversight of the progress by Indian Point Unit 2 Power Plant (IP2) toward fulfilling commitments made to NRC in 1997 regarding design bases requirements. These commitments were intended to improve plant programs and processes for controlling and maintaining reactor operations. OIG also reviewed the adequacy of NRC oversight of the licensee regarding the implementation of these commitments.

As a result of the inquiry OIG found that NRC's oversight of IP2's efforts toward fulfilling design bases requirements was adequate. OIG found that NRC dedicated significant resources to intensify regulatory oversight of the plant. However, despite heightened levels of NRC attention to plant weaknesses, problems at IP2 remained unresolved. NRC considered the licensee's progress towards meeting commitments for plant improvement to be slow and limited in effectiveness.

- OIG conducted an investigation into an allegation that the National Institute of Standards and Technology (NIST), while performing an analysis of the Baltimore, MD tunnel fire of July 18, 2001 for the NRC,

*(continued on next page)*

was influenced by NRC staff to develop test results that supported the regulatory standards used by NRC in its certification of spent fuel shipping casks.

OIG learned that in February 2002, NRC contracted with NIST to simulate the fire created in the Baltimore, MD tunnel fire to determine if the thermal environment created during the tunnel fire would have exceeded the performance standard contained in NRC's certification of spent fuel shipping casks. OIG determined that the NRC staff did not influence the study.

- OIG conducted an investigation into an allegation that an NRC intern inspector

submitted a fraudulent receipt for lodging as part of the inspector's official travel voucher pertaining to a 2-month temporary assignment.

OIG determined that in November 2002, the inspector submitted a fraudulent sublet contract agreement to the regional travel office to obtain reimbursement from NRC for compensation improperly paid to a friend with whom the inspector resided during the temporary assignment. OIG also determined that the inspector used the Government-issued Citibank Visa travel card to obtain \$4,388 in unauthorized cash withdrawals. NRC allowed the inspector to resign from employment at NRC.

---

# THE OFFICE OF THE INSPECTOR GENERAL

## **HISTORY OF THE INSPECTOR GENERAL ACT**

October 12, 2003, marked the 25<sup>th</sup> anniversary of the enactment of the Inspector General Act. On October 12, 1978, the President created independent audit and investigative offices in 12 Federal agencies. Before that time, most Federal audit and investigative resources were under the management of specific Federal program offices — meaning that Federal auditors and investigators were frequently under the direction of the programs they were reviewing. This fragmented system also made it hard for these small audit and investigative offices to see patterns of abuse in their agencies' programs. The need for that independent review remains the solid foundation that guides the Inspector General (IG) community today.

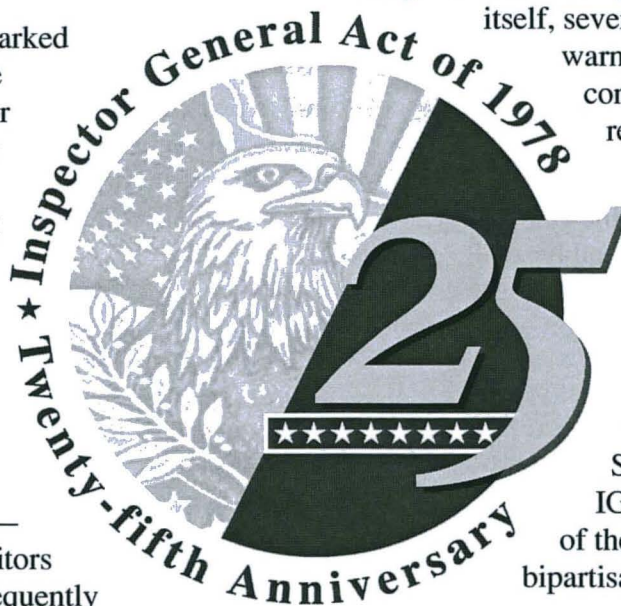
Establishing the IG concept into law required considerable time and effort. Work in the early 1960s by a U.S. House of Representatives subcommittee of the Government Operations Committee, began to highlight the need for independent statutory IGs. Further work by this subcommittee in 1974 revealed a situation in the former Department of Health, Education, and Welfare (HEW) where processes for investigating program fraud and abuse were essentially non-existent. In

response, legislation establishing a statutory IG at HEW was enacted 2 years later. During congressional hearings debating the IG Act

itself, several witnesses sounded warnings of serious adverse consequences that would result if the IG Act became

law and others questioned the constitutionality of some of the IG Act's provisions. However, these concerns were tempered by the testimony of the HEW Secretary and IG, and the IG Act passed both houses

of the Congress with strong bipartisan support.



Now, 25 years later, it is clear that the basic tenets of the IG Act's intended mission have remained constant and strong. The act has been amended several times over the years to add new IGs and clarify reporting requirements. The IG Act has given IGs the authority and responsibility to be independent voices for economy, efficiency, and effectiveness within the Federal Government. Today 57 IGs protect the integrity of Government, improve program efficiency and effectiveness, and prevent and detect fraud, waste, and abuse in 59 Federal agencies which includes 29 Presidentially appointed Inspectors General. The IG at NRC and those at other Federal agencies are appointed by the President and confirmed by the Senate. The remainder are appointed by their respective agency head.

*(continued on next page)*

Since their early beginnings, IGs have focused attention on good government. Individual Offices of Inspector General view themselves as “agents of positive change” within their agencies and direct their work toward program efficiency and effectiveness and the protection of government integrity. IGs endeavor to be influential forces in identifying vulnerabilities in their agency’s programs and operations and facilitating solutions, and leveraging their resources to promote Government integrity, accountability, transparency, and excellence. While changes in vulnerability and risk have affected the focus of their work and priorities over the years, IG offices have drawn on their broad base of knowledge and expertise to adapt to these changes and remain relevant and on point.

The IG concept has proven to be of significant benefit to our Government. IG investigations contribute to the prosecution of thousands of wrongdoers and recovery of billions of dollars annually. In fiscal year (FY) 2001 alone, IGs were responsible for more than \$28 billion in saved and recovered Federal funds.

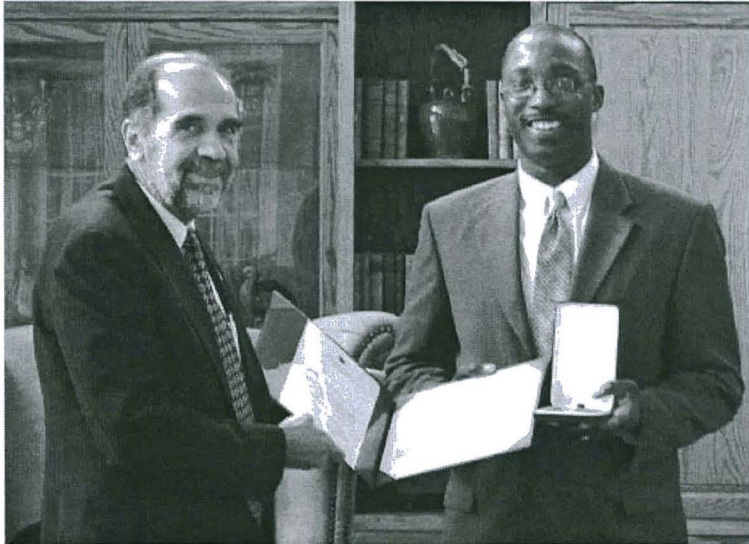
Over the last several years, IGs have operated in a changing environment. IGs are now playing a pivotal role within their agencies by conducting financial audits, reporting on Government Performance and Results Act compliance and accountability, assessing information security efforts, identifying their agencies’ most significant challenges, and reviewing the effective implementation of the President’s Management Agenda. Helping to fight terrorism, evaluating the Nation’s critical infrastructure, striving to improve the Government’s financial management, and validating agency performance and accountability measures are among the key tasks facing the Nation’s IGs today. These tasks have emerged as a result of the priorities established by the Administration or the Congress and, more recently, threats against our homeland.

The Presidentially appointed IGs work together and coordinate their professional activities through the President’s Council on Integrity and Efficiency (PCIE). A like organization, the Executive Council on Integrity and Efficiency (ECIE), is comprised primarily of the IGs appointed by designated Federal entity heads. Both the PCIE and ECIE were created by Executive Order in 1981 and 1992, respectively, and were charged with addressing integrity and efficiency issues that transcend individual Government agencies and increasing the professionalism and effectiveness of IG office personnel throughout Government. Through their committees and working groups, both Councils have addressed relevant issues related to audit, investigation, and inspection efforts; developed professional standards, guidelines, and manuals; issued reports on Governmentwide initiatives and concerns; and trained IG staff to remain current in their respective professions.

Congress established the NRC Office of the Inspector General (OIG) through a 1988 amendment to the IG Act. Today, OIG’s primary mission is to assist NRC by ensuring integrity, efficiency, and accountability in the agency’s programs to regulate the civilian use of byproduct, source, and special nuclear materials in a manner that adequately protects the health and safety of the public, as well as the environment, while promoting the Nation’s common defense and security. In FY 2003, the NRC’s total budget authority was \$585 million, which included a \$6.8-million appropriation for OIG.

## **ORGANIZATION AND FUNCTIONS OF NRC’S OIG**

NRC’s OIG includes auditors, criminal investigators, legal counsel, and a resource management and operations (RMOS) staff. OIG’s audit program is designed to provide assurance to the Chairman and to Congress that



*Hubert T. Bell, Inspector General at the U.S. Nuclear Regulatory Commission presents Special Agent Malion A. Bartley (right) with the United States Air Force Meritorious Civilian Service Award. As leader of the Air Force Office of Special Investigations Surveillance Detection Team, Mr. Bartley distinguished himself by conducting operations that greatly protected the safety of personnel in high threat areas from foreign intelligence services and terrorism.*

NRC programs and operations are working efficiently and effectively. Consequently, the audit staff conducts performance and financial audits as well as special evaluations. Performance audits focus on NRC's administrative and programmatic operations. Financial audits focus on NRC's internal control systems, transaction processing, and financial systems. In special evaluations, OIG auditors present OIG perspectives or information on specific topics.

The mission of OIG's investigative program is to perform investigative activities related to the integrity of NRC's programs and operations. The majority of OIG's investigations focus on allegations of fraud, waste, and abuse and violations of law or misconduct by NRC employees and contractors. Additionally, OIG investigates allegations of irregularities or abuses in NRC programs and operations with special emphasis on those NRC activities that could adversely impact public

health and safety. As a complement to the investigative function, the investigative staff also conducts Event Inquiries, which yield reports documenting the examination of events or agency regulatory actions that do not specifically involve individual misconduct. Instead, these reports identify staff actions that may have contributed to the occurrence of an event. In addition, OIG issues special inquiry reports that document instances where OIG has identified inadequacies in NRC regulatory oversight that may result in a potential adverse impact on public health and safety.

OIG's General Counsel (GC) provides independent legal advice on issues concerning criminal law and procedures, evidence, and constitutional law as they relate to OIG's investigative program. The GC also develops legal interpretations of appropriations law, financial management statutes and regulations, and procurement and funding rules in support of OIG's audit program. In addition, the GC conducts and coordinates, with other cognizant OIG staff, in-depth reviews of existing and proposed legislation, regulations, and agency directives that affect NRC programs and operations and, as appropriate, provides written comments. The intent of these reviews is to assist the agency in identifying and preventing potential problems.

The RMOS staff formulates and executes the OIG budget, prepares OIG's *Semiannual Report* to Congress, operates an independent human resources management program, administers the control of OIG funds, administers OIG's information technology program, coordinates strategic planning activities, and performs a variety of other support functions.



---

# THE NUCLEAR REGULATORY COMMISSION

## REGULATOR OF NUCLEAR SAFETY

NRC was formed in 1975 to regulate the various commercial and institutional uses of nuclear energy, including nuclear power plants. The agency succeeded the Atomic Energy Commission, which previously had responsibility for both developing and regulating nuclear activities. NRC's mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear material 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; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear material and waste.

Under its responsibility to protect public health and safety, NRC has three principal regulatory functions: (1) establish standards and regulations, (2) issue licenses for nuclear facilities and users of nuclear materials, and (3) inspect facilities and users of nuclear materials to ensure compliance with the requirements. These regulatory functions relate to both nuclear power plants and other uses of nuclear materials — like nuclear medicine programs at hospitals, academic activities at educational institutions, research work, and such industrial applications as gauges and testing equipment.

NRC has recognized the need to keep the public informed of its work. The agency maintains a current Web site and a public

document room in its headquarters and holds public hearings and public meetings in local areas and at NRC offices, and discussions with individuals and organizations.

### **WHY NRC REGULATES**

The nuclear industry is strictly regulated because of the potential hazards involved in using radioactive materials. These radioactive materials release radiation, which can be hazardous to people if they are exposed to it in significant amounts. The extent of the risk depends on the type and amount of radiation emitted by the radioactive material, the distance between the source of the radiation and a person, and the length of time a person is exposed to the radiation.

The risks can be lessened by reducing any or all of these factors. The hazard is less if there are shielding materials like lead or concrete to block some of the radiation, if a person moves farther away from the radiation source, or if the exposure time is reduced.

If radioactive materials are properly handled and regulated, they do not pose a significant risk to the public or to workers.

Radioactivity from natural sources is present throughout the world. People are continuously exposed to low-level radiation from radioactive materials in the earth and

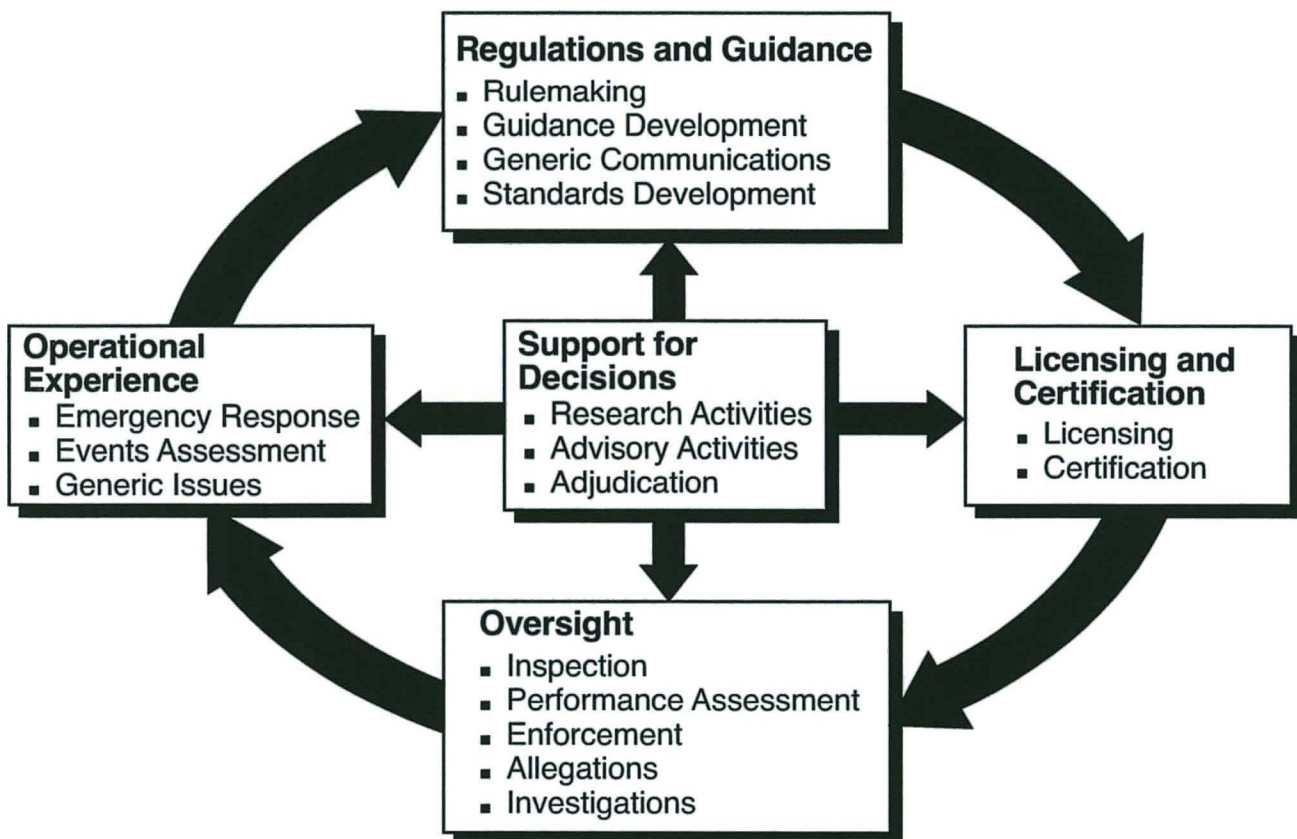
*(continued on next page)*

cosmic rays from space. Exposure to natural radiation can be affected by geography as well as lifestyle. For example, radiation levels are higher in the mountains, and travel by airplane increases exposure because of greater cosmic radiation at high altitudes. Most people also receive some radiation exposure from medical and dental x-rays and other medical procedures.

NRC's regulatory program established limits for radiation exposure to workers and the general public as a result of the various uses of radioactive materials licensed by NRC. In addition, NRC requires users to take steps to keep exposures well below the limits.


## HOW NRC REGULATES

The diagram gives an overview of NRC's regulatory process. This process has five main components: (1) developing regulations and guidance for its applicants and licensees, (2) licensing or certifying applicants to use nuclear materials or operate nuclear facilities, (3) overseeing licensee operations and facilities to ensure that licensees comply with safety requirements, (4) evaluating operational experience at licensed facilities or involving licensed activities, (5) conducting research and holding hearings to address the concerns of parties affected by agency decisions, and obtaining independent reviews to support its regulatory decisions.





## MANAGEMENT CHALLENGES FACING NRC IDENTIFIED BY OIG

NRC's Most Serious Management Challenges as of November 18, 2002	
<p><b>Challenge 1</b> Protection of nuclear material and facilities used for civilian purposes.</p>	<p><b>Challenge 6</b> Intra-agency communication (up, down, and across organizational lines).</p>
<p><b>Challenge 2</b> Development and implementation of an appropriate risk-informed and performance-based regulatory oversight approach.</p>	<p><b>Challenge 7</b> Integration of regulatory processes in a changing external environment.</p>
<p><b>Challenge 3</b> Acquisition and implementation of information resources.</p>	<p><b>Challenge 8</b> Maintenance of a highly competent staff (i.e., human capital management).</p>
<p><b>Challenge 4</b> Administration of all aspects of financial management.</p>	<p><b>Challenge 9</b> Protection of information.</p>
<p><b>Challenge 5</b> Clear and balanced communication with external stakeholders.</p>	<p> The challenges are <i>not</i> ranked in any order of importance.</p>



---

# THE AUDIT PROGRAM

*To help the agency improve its effectiveness during this period, the OIG completed one financial and nine performance audits that resulted in a number of recommendations to NRC management. OIG analyzed eight contract audit reports, two of which identified \$205,396 in questioned costs.*

## AUDIT SUMMARIES

### ***Computer Security Reviews at NRC's Region I, Region II, Region III, and Region IV***

These reports describe the results of OIG's computer security reviews at NRC's regional offices located in King of Prussia, Pennsylvania (Region I); Atlanta, Georgia (Region II); Lisle, Illinois (Region III); and Arlington, Texas (Region IV).

Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, requires agencies to implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. The Federal Information Security Management Act (FISMA) of 2002 outlines the information security management requirements for agencies. These requirements include an independent evaluation of an agency's information security program and practices and an evaluation of the effectiveness of information security control techniques. The FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines.

The security reviews found that the controls implemented by the regions are

generally effective in reducing the risks associated with their operations. However, several areas need improvement. These areas include administrative security controls, information technology controls, physical security controls, safety controls, and supporting utilities. Because the reports contain sensitive unclassified information, the details of the areas needing improvement are not available for public dissemination. (*Addresses Management Challenge #9*)

### ***Audit of NRC's Regulatory Oversight of Special Nuclear Materials***

NRC is authorized to grant licenses for the possession and use of special nuclear material (SNM) and establish regulations to govern the possession and use of those materials. Practical uses of SNM include (1) fuel for nuclear reactors; (2) industrial, academic, and medical research and testing; and (3) the manufacture of industrial gauging devices (sealed sources). NRC's Commission states that proper control and accounting of SNM is an important component of the agency's safeguards and security programs.

NRC's regulations require that certain materials licensees have extensive material control and accountability (MC&A) programs as a condition of their license. However, all

*(continued on next page)*



Special Nuclear Material – Cesium-37 gamma irradiation source

license applicants, including those requesting authorization to possess small quantities of SNM, must develop and implement plans and activities that demonstrate a commitment to accurately control and account for radioactive materials. Licensees are also required to allow NRC to inspect the materials, controls, and premises where SNM and source materials are used or stored. Additionally, NRC requires that materials licensees report information to the Nuclear Materials Management and Safeguards System (NMMSS). NMMSS is a computer database managed by the U.S. Department of Energy (DOE) and jointly used with NRC as the national system for tracking certain private- and Government-owned nuclear materials.

Today's heightened sensitivity to the control of SNM warrants NRC's serious attention to its licensees' material control and accounting activities. NRC performs limited inspections of licensee MC&A activities, and cannot assure the reliability of the SNM

tracking system. NRC's current levels of oversight of licensee MC&A activities do not provide adequate assurance that all licensees properly control and account for SNM.

Without adequate inspections to verify licensee commitments to MC&A, or a reliable SNM tracking system, NRC has no independent means for determining if SNM was lost, stolen, or otherwise diverted while in a licensee's possession. Despite not being a regulatory requirement, having this independent ability would enhance the agency's oversight abilities. (Addresses Management Challenges #1, 3, 5)

### ***Audit of NRC's Oversight of Research and Test Reactors***

Research and test reactors (also called non-power reactors) are nuclear reactors whose primary function is the safe conduct of research and development activities. Almost every field of science makes use of these reactors, which are also used to educate students for careers in the nuclear power industry, national defense, and research. The NRC currently licenses 50 research and test reactors. Thirty-five of those are operating in 23 States. Fifteen others are no longer operating and are being decommissioned.

In contrast to commercial nuclear power facilities, most non-power reactors are located in urban areas, with the majority located on university campuses. The facilities typically range in power output from 0.10 watts to 20 megawatts (thermal) and most produce less than 1/1000 the power of a commercial power reactor. Unlike commercial power plants, facility staff regularly work in the reactor room or building during operation.

Radiation produced by the reactor is used in a variety of research activities at non-power reactor facilities. For example, non-power reactors are routinely used to precisely measure

---

the presence of trace elements like environmental pollutants in soil, water, air, and foods. They are also used in the production of radiopharmaceuticals and the development of treatments for shrinking cancerous tumors.

Oversight of research and test reactors was meeting NRC's expectations. Staff met goals for reviewing and approving licensee requests for changes to their licenses and approving licensee demand to license reactor operators. In addition, inspection requirements were generally satisfied.

However, some aspects of oversight can be improved. Specifically, NRC can (1) improve guidance for inspection followup items to describe for *licensees* what an inspection followup item means in regulatory terms, (2) improve operating plans to represent a discrete level of activity so that management can monitor performance and resource usage, (3) increase the availability of information so that the public can effectively participate in or make reasonable judgments about the adequacy of NRC's research and test reactor inspection program, and (4) document inspector training so that employee training records show compliance with training requirements. (*Addresses Management Challenges #1, 2, 7*)

#### ***Memorandum Report: Review of NRC's Purchase Order Processing***

OIG is conducting an audit of NRC's contract administration practices during which it reviewed NRC's purchase order processing. OIG issued an interim report which identified a process improvement opportunity which suggested discontinuing the use of overlapping standalone systems. Agency offices have non-integrated computer systems, that require entry of the same or similar information. This condition exists because NRC has not developed an integrated system that meets the needs of its

Division of Contracts, Division of Financial Management, and the program offices. The contracting and accounting organizations recognized this problem and both organizations are currently working together to develop an integrated E-Procurement System. In addition, action has been initiated to make process improvements in the commercial payments area. Close intra-agency coordination on these initiatives will contribute significantly to the success of the initiatives as well as (1) foster implementation of the Government Paperwork Elimination Act, (2) support the President's E-Government initiatives, (3) result in net savings of more than \$338,000 over a 5-year period, and (4) facilitate compliance with recent Joint Financial Management Improvement Program Acquisition/Financial Systems Interface Requirements. (*Addresses Management Challenge #4*)

#### ***Closeout Audit of GSE Power Systems, Inc.***

This report reflects the results of the review to determine the allowability and allocability of the direct and indirect costs claimed in the closeout documents. The audit disclosed that GSE did not maintain sufficient records to fully support contract costs, which is a failure to comply with the requirements of Federal Acquisition Regulation (FAR) 52.215-2, *Audit Records - Negotiation*, which is incorporated in the contract by reference. The audit also recommended disallowances totaling \$97,758 in contract costs. (*Addresses Management Challenge #4*)

#### ***Memorandum Report: Followup Review of NRC's Internet Usage***

OIG conducted a followup audit on Internet use to assess corrective actions related to a prior report (October 2001). That

*(continued on next page)*

assessment found that 52 percent of agency employee Internet activity was for personal use. Approximately 5 percent of the personal use, including looking at sexually explicit Web sites, was in direct violation of NRC policy. At the time, OIG said that because of the amount of personal use and the occurrences of prohibited use, the agency needed to enforce its policy regarding personal Internet usage.

The NRC promptly implemented corrective actions.

The followup audit showed that in January 2003, 51 percent of NRC employee Internet activity was for personal use (compared to 52 percent in 2001). Prohibited activity decreased from 5 percent in 2001 to less than 1 percent in 2003.

That visits to these types of Web sites still occur is significant because the agency blocks them. NRC does this because it considers this prohibited activity to constitute egregious misconduct, in part because the contents may be offensive to others and could lead to potential legal liabilities for the agency. Because the total amount of personal use remains over 50 percent, the agency needs to take further action to manage employees' personal use of the Internet at NRC. (*Addresses Management Challenges #3, 6*)

### ***Evaluation of NRC's Implementation of the Federal Information Security Management Act for FY 2003***

OIG audited the NRC's information security program in accordance with the requirements of the Federal Information Security Management Act (FISMA). The objectives of the evaluation were to (1) test the effectiveness of information security policies, procedures, and practices of a representative

subset of the agency's information systems and (2) assess compliance with the FISMA and related information security policies, procedures, standards, and guidelines.

Over the past year, NRC made progress in improving its security program and in implementing the corrective actions from the 2002 Government Information Security Reform Act review. For example, NRC completed all of the required security documents for the Major Applications (MA) and General Support Systems (GSS) currently in production, increasing the overall levels of security for the systems; certified and accredited all MAs and GSSs currently in production; conducted several security reviews including a Foreign Network Vulnerability Assessment; improved management tools and repositories used to track, control, and protect security documentation and track completion of corrective actions; and completed a majority of corrective actions from the previous review. However, several areas need improvement.

First, NRC's Operating and System Software Maintenance Procedures are not followed consistently, contributing to an incomplete inventory of NRC operating and system software. Second, new weaknesses and corrective actions identified during the past fiscal year were not always added to the system that tracks corrective actions. Third, recent computer security reviews of the four NRC regional offices found systems on NRC's master inventory that do not meet the criteria for inclusion on the list, or are no longer being used. The inventory is currently being reviewed and updated to ensure that only those systems that meet the criteria defined in MD 12.5 are included. (*Addresses Management Challenges #3, 9*)

---

## **AUDITS IN PROGRESS**

### ***Audit of NRC's FY 2003 Financial Statements***

Under the Chief Financial Officers Act and the Government Management and Reform Act, OIG is required to annually audit the financial statements of the NRC. 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 measure the agency's improvements by assessing corrective action taken on the prior year's audit findings. *(Addresses Management Challenge #4)*

### ***Audit of NRC's Management of the Acquisition Process***

During FY 2002, NRC executed approximately \$96 million in contract actions for Division of Contracts (Contracts) activities alone. Additional funds are obligated for contract vehicles outside the realm of Contracts. Contracts is responsible for (1) developing and implementing agencywide contracting policies and procedures and (2) providing advice and assistance to NRC program officials regarding the NRC Acquisition Regulation, Federal Acquisition Regulations, and methods for meeting program objectives consistent with such regulations. To meet the needs of agency contract management personnel, Contracts, in conjunction with the Office of Human Resources, developed the agency's acquisition training curriculum. The curriculum includes both mandatory and recommended modules and

focuses on the entire NRC acquisition process. This review is evaluating whether NRC provides adequate oversight of (1) the contracting process and (2) training for the acquisition workforce. *(Addresses Management Challenge #4)*

### ***Special Evaluation of NRC's Most Serious Management Challenges (FY 2004)***

In January 2000, Congress enacted the *Reports Consolidation Act of 2000* to provide financial and performance management information in a more meaningful and useful format for Congress, the President, and the public. Included in the act is the requirement that each Federal agency IG summarize what he or she considers to be the most serious management and performance challenges facing his or her respective agency and assess the agency's progress in addressing those challenges. This special evaluation satisfies the congressional requirement.

The overall objectives for this evaluation are to assess the agency's efforts to address the management challenges and to identify any related agency programs that have had questionable success in achieving results. This evaluation will help OIG update the annual list to Congress of NRC's most serious management challenges, which is usually due in December. This evaluation is performed annually. *(Addresses All Management Challenges)*

### ***Audit of NRC's Personnel Security Program***

NRC's personnel security program makes determinations on the initial and continuing eligibility of NRC applicants, consultants, and employees for facility access authorizations, employment clearances, and access to restricted data and national security information. The

*(continued on next page)*

program also makes determinations on the initial and continuing eligibility of contractor employees for building access and for access to sensitive information technology systems and data. This audit continues audit work performed during FY 2003 on this issue. In FY 2003, auditors focused on the personnel security process as it pertains to contractor employees. During FY 2004, auditors are focusing on other program components to determine whether the program is effectively managed and achieves its goals. (*Addresses Management Challenge #9*)

### ***Audit of NRC's Protection of Safeguards Information***

Safeguards information is sensitive unclassified information that specifically identifies the detailed (1) security measures of a licensee or an applicant for the physical protection of special nuclear materials or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. NRC established its Sensitive Unclassified Information Security Program to ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure under pertinent laws, management directives, and applicable directives of other Federal agencies and organizations. This audit is assessing whether NRC's program (1) adequately ensures the protection of safeguards information, (2) prevents the inappropriate release of safeguards information to the public and NRC employees who should not have access, and (3) adequately defines what constitutes safeguards information. (*Addresses Management Challenge #9*)

### ***Audit of NRC's Incident Response Program***

In response to an event at an NRC-licensed facility that could threaten public health and safety or the environment, NRC activates its incident response program at its Headquarters Operations Center and one of its four Regional Incident Response Centers. NRC's highest priority is to provide expert consultation, support, and assistance to State and local public safety officials responding to the event. Once the incident response program is activated, teams of specialists are assembled at the Headquarters Operations Center and respective Regional Incident Response Center to obtain and evaluate event information and to assess the potential impact of the event on public health and safety and the environment. Communications with the news media, State, other Federal agencies, the Congress, and the White House are coordinated through the Headquarters Operations Center. Because NRC's incident response program is critical to the agency's mission to ensure adequate protection of public health and safety, this audit will assess if this program is operating effectively and efficiently. (*Addresses Management Challenge #1*)



*NRC's Incident Response Center*



---

### ***Audit of the Baseline Inspection Program***

Beginning in FY 2001, the Reactor Inspection Program and the Reactor Performance Assessment program were combined into a single program for commercial power reactors. The combined program, the revised Reactor Oversight Program, includes risk-informed baseline inspections, use of performance indicator data, and a revised reactor assessment process. The program is designed to ensure, through selective examinations, that the licensee identifies and resolves safety issues before they affect safe plant operations.

Baseline inspections provide for increased focus on aspects of performance that have the

greatest impact on safe plant operation. The level of plant-specific inspection performed at each site is commensurate with that site's performance. The program is an integral part of the NRC's reactor oversight process, provides a mechanism for NRC to remain alert to plant status and conditions at all licensed reactors, and supports the goals and objectives of the reactor oversight process.

This audit is assessing whether the baseline inspection program: (1) is based on a sound methodology, (2) is being completed at all commercial power plants, and (3) has sufficient resources available to carry out the program. (*Addresses Management Challenges #1, 2*)



---

# THE INVESTIGATIVE PROGRAM

*During this reporting period, the OIG received 156 allegations, initiated 32 investigations, and closed 52 cases, 2 Event Inquiries, and 1 special project. In addition, the OIG made 31 referrals to NRC management. These investigations resulted in \$73,527 in recoveries and \$421,000 in cost savings to the Federal Government.*

## **INVESTIGATIVE CASE SUMMARIES**

### ***Adequacy of NRC Oversight Related to Reactor Vessel Leakage at Oconee and North Anna Nuclear Power Stations***

OIG completed an Event Inquiry into NRC's regulatory oversight of the operations at the Oconee and North Anna Nuclear Power Stations relating to the leakage from the reactor pressure vessel (RPV) head. The OIG received allegations that between Spring 2001 and Spring 2003, NRC allowed Oconee Units 1, 2, and 3 and North Anna Unit 1 to operate with known or suspected RPV head leakage in violation of plant technical specifications and that NRC took no enforcement action against the licensees for those violations. The RPV head typically contains 65 to 70 holes (penetrations) into which vertical tubes called vessel head penetration nozzles are placed. The allegation cited one penetration (#50) in the RPV head as an example of known leakage at North Anna Unit 1.

As a result of this inquiry, OIG found no evidence that the NRC staff permitted the licensees of Oconee or North Anna power plants to operate with known or suspected leakage of the RPV head. Specifically, OIG learned that the licensees for Oconee and North Anna utilized acceptable techniques during outages to

inspect for cracking and leakage. In each case where leakage was discovered during plant outages, the NRC staff reviewed licensees' repairs and determined that the repairs were appropriately implemented. Additional RPV leakage found during subsequent outages were repaired before restarting the plants.

OIG also determined that in spite of NRC staff efforts to ensure that the Oconee and North Anna power plants did not operate with known or suspected RPV leakage, Penetration #50 at North Anna Unit 1 may have leaked for an entire operating cycle (Fall 2001 - Spring 2003). The NRC staff acknowledged that both the licensee and NRC staffs were probably mistaken in their conclusion (during the September 2001 outage) that the leakage at Penetration #50 was not from a flaw. However, OIG found that in the Fall 2001, when North Anna Unit 1 restarted, neither the licensee nor NRC staffs had any evidence of ongoing leakage from this penetration.

In addition, OIG learned that because of the potential for continuing RPV leakage, both units at North Anna replaced their vessel heads. Oconee Unit 3 also recently completed the replacement of its vessel head, and Units 1 and 2 are scheduled for vessel head replacement in Fall 2003 and Spring 2004, respectively.  
*(Addresses Management Challenge #1)*

*(continued on next page)*

### ***Misuse of the NRC Full Share (Transportation Subsidy) Program***

OIG conducted a proactive review of the NRC Full Share Program to identify potential deficiencies in the administration of the program. The NRC Full Share Program provides a transportation subsidy benefit to eligible Government employees who use public transportation or a van pool for their regular, daily, and direct commute between home and work. As a result of information developed during the review, OIG completed three investigations that substantiated NRC employee misuse of the transportation subsidy program.

As a result of these investigations, OIG found that one NRC employee deliberately misused the program subsidy by giving his subsidy totaling \$1,075.90 to a personal friend, and another NRC employee falsely certified two applications for the program when he listed a home address that he did not use as his daily direct commute from home to work and return. This NRC employee received \$2,522 in transportation benefits which he was not entitled to receive. A third NRC employee, who claimed he resided in Washington, DC when in fact he resided in Rockville, MD, received \$905 in benefits to which he was not entitled. This employee also misused the subsidy program by using the Full Share Program farecard when he was not at work. NRC recovered the farecards whose value totaled \$2,522. (*Addresses Management Challenge #4*)

### ***Early Retirement Under False Pretenses***

OIG completed an investigation into an allegation that a former employee was provided Discontinued Service Retirement (DSR) to which he was not entitled. According to the information received by OIG, the employee, who was under consideration for termination as a result of misconduct, received a DSR from the

NRC after declining to be reassigned outside of his commuting area. There was no proof that the employee was actually offered a legitimate position outside of his commuting area, the declination of which purportedly qualified him for the DSR.

This investigation disclosed that NRC entered into a settlement agreement with the employee which improperly provided the employee a DSR. According to U.S. Office of Personnel Management (OPM) retirement regulations, an employee who is terminated for engaging in misconduct is not eligible to receive a DSR. OIG found that an NRC official fabricated a directed reassignment to a nonexistent position which allowed the employee to decline the reassignment and to qualify for the DSR without regard to the employee's misconduct. OPM directed the employee to repay the Government the annuity he had already received in the amount of \$61,456.63. In addition, as a result of this investigation, until the employee is eligible for a deferred annuity, the Government will realize a future cost savings of \$421,100 (absent future cost of living increases) which would have been paid to the employee. (*Addresses Management Challenge #4*)

### ***Misuse of NRC Computers To Access Pornographic Material***

OIG completed a proactive review for fiscal years 2001 through 2003 to identify the potential misuse of information technology resources by NRC employees and contractors. This review centered on the network activity passing through the NRC's primary conduit to the Internet and identified NRC computers requesting and receiving materials from Web sites containing sexually explicit materials. The preliminary information was confirmed using computer forensic methods and resulted in 30 investigations of NRC employees and contractors.

---

As a result of the investigations, OIG found that 22 NRC employees and 7 contractor employees were routinely accessing sexually explicit Internet sites from their assigned NRC computers. Each of the subjects of these investigations confessed to their activities and, furthermore, each indicated they were aware of the NRC's policies against accessing such materials. Responsive action taken by NRC toward its employees ranged from a 21-day suspension to job termination.

Additionally, OIG discovered that the NRC contract guard force was misusing their Internet access on computers provided by the NRC in violation of specific provisions within their contract with the NRC. The NRC is currently negotiating with the contract guard force and a contractor providing computer services to deduct the value of the hours lost to these unapproved and non-contract related activities which has been estimated at over \$17,000. (*Addresses Management Challenge #3*)

### ***NRC Enforcement of Regulatory Requirements and Commitments at Indian Point, Unit 2***

The OIG initiated this Event Inquiry (EI) in response to a Congressional request that OIG examine issues concerning NRC oversight of operations at the Indian Point Unit 2 (IP2) power plant in Buchanan, NY. Specifically, the EI examined NRC's oversight of IP2's progress toward fulfilling two design bases commitments made to the NRC in 1997 to initiate and complete an Updated Final Safety Analysis Report (UFSAR) review program and to update existing design basis documents (DBD); NRC's response to the specific concerns raised by an IP2 engineering consultant pertaining to discrepancies between design drawings and the as-built configuration of the Reactor Protection

System (RPS); NRC's oversight of IP2's corrective action program between 1995 and 2001; and NRC's utilization of its Senior Management Meeting process to heighten attention to IP2.

As a result of this EI, OIG found that the NRC considered the licensee's progress towards meeting 1997 commitments for a UFSAR review program and to update DBDs to be slow and limited in effectiveness. OIG determined that NRC responded appropriately to the concerns raised by an IP2 engineering consultant who raised the issue that collectively the RPS wiring discrepancies warranted a higher level of attention than the licensee had determined was appropriate. The NRC conducted three inspections relative to these issues and also validated some of the concerns the consultant had raised. Between 1995 and 2001, IP2 experienced a series of operational problems attributed in part to deficiencies in IP2's corrective action program. OIG learned that between 1995 and 2001, NRC conducted 20 special team inspections, logging thousands of hours dedicated to engineering and problem identification and resolution. Additionally, OIG learned that NRC issued 13 enforcement actions to IP2 during this time frame. OIG determined that in spite of intensified regulatory oversight by NRC, IP2 was able to achieve only limited improvement in plant performance. OIG found that the NRC Region I Administrator attempted during the Senior Management Meeting process on four occasions between 1997 and 2000 to have NRC's senior managers place IP2 on the agency's Watch List. OIG agreed with the Region I Administrator that placing IP2 on the Watch List sooner might have sufficiently motivated the licensee to cause earlier improved performance. (*Addresses Management Challenge #1*)

*(continued on next page)*

### ***Improper Influence by NRC Staff on Results of NIST Test***

OIG conducted an investigation into an allegation that the National Institute of Standards and Technology (NIST), while performing an analysis of the Baltimore, MD tunnel fire of July 18, 2001 for NRC, was influenced by NRC staff to develop test results that supported the regulatory standards used by the NRC in its certification of spent fuel shipping casks.

The allegation specified that NIST was “being leaned on” by NRC to produce specific test results which would support NRC’s regulatory standards in the performance of spent fuel shipping casks. The regulatory standards specified that the spent fuel shipping casks sustain thermal temperatures of up to 1,475 degrees Fahrenheit.

OIG learned that in February 2002, NRC contracted with NIST to simulate the conditions created in the Baltimore tunnel fire to determine if the thermal environment created by the tunnel fire would have exceeded the performance standards contained in the NRC certification of spent fuel shipping casks. OIG interviewed NIST and NRC employees. NIST employees asserted that NRC staff never attempted to influence the direction of the study and that there never was any indication that NRC wanted a desired result. Temperatures of the fire simulated by NIST did exceed 1,475 degrees Fahrenheit in the hottest area of the fire near the tunnel ceiling; however, this temperature was

not exceeded at the location of the spent fuel shipping cask. OIG determined that NRC did not attempt to influence the study. (*Addresses Management Challenge #2*)

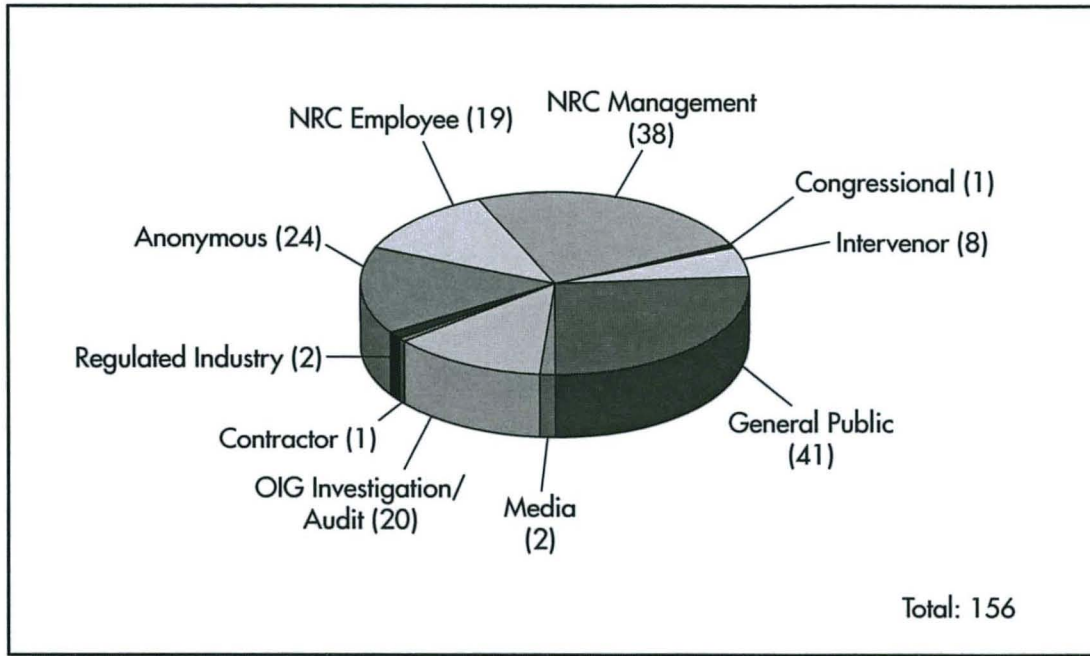
### ***Fraudulent Travel Claim by NRC Employee***

OIG conducted an investigation into an allegation that an NRC intern inspector submitted a fraudulent receipt for lodging as part of the inspector’s official travel voucher pertaining to a 2-month temporary assignment.

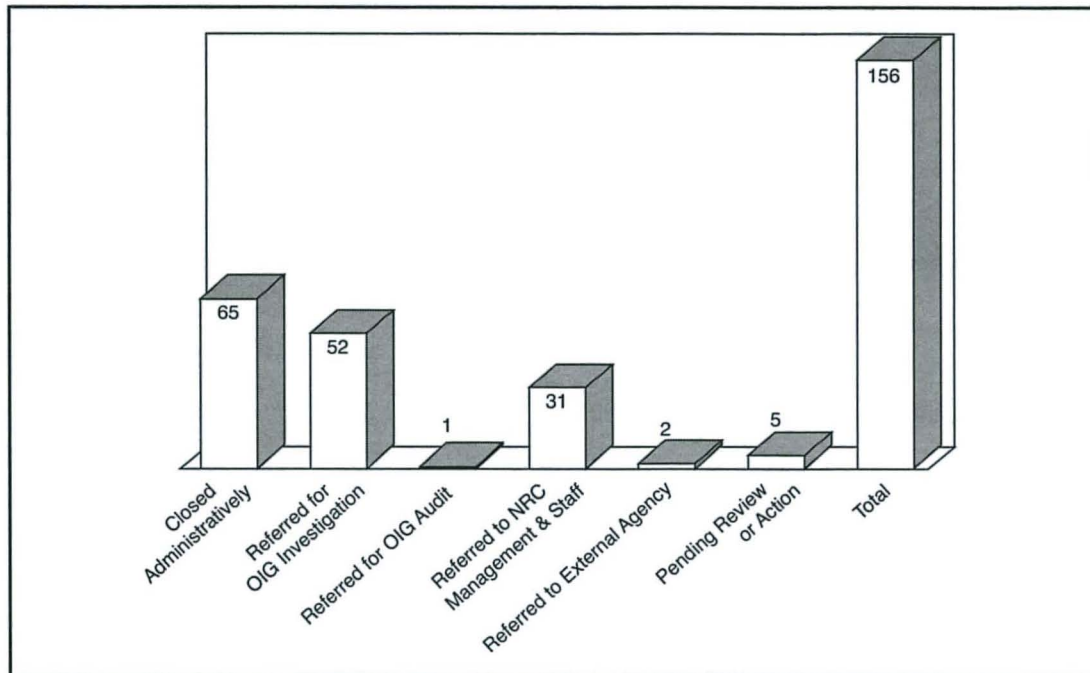
OIG determined that in November 2002, the inspector submitted a fraudulent sublet contract agreement to the regional travel office to obtain \$1,400 reimbursement from NRC for compensation improperly paid to a friend with whom the inspector resided during the temporary assignment. OIG determined that between August 22, 2001, and November 10, 2002, the inspector used the Government-issued Citibank Visa travel card 18 times to obtain unauthorized cash withdrawals totaling \$4,388.25. OIG determined that between June 25, 2001, and April 13, 2003, the inspector was delinquent in paying his/her monthly Citibank account 10 times. The past due amounts on the account ranged from \$781.05 to \$4,098.40. OIG also determined that between October 12, 2001, and November 25, 2002, the inspector wrote five non-sufficient funds checks totaling \$11,849.34 in payments to the Citibank account. NRC allowed the inspector to resign from employment at NRC. (*Addresses Management Challenge #4*)

## INVESTIGATIVE STATISTICS

### Source of Allegations — April 1, 2003, through September 30, 2003



### Disposition of Allegations — April 1, 2003, through September 30, 2003



### Status of Investigations

DOJ Referrals	16
State Referrals	1
DOJ Declinations	16
State Declinations	1
Indictments and Arrests	1
Recoveries	\$73,527
Cost Savings to the Federal Government	\$421,000
NRC Administrative Actions:	
Terminations and Resignations	7
Suspensions and Demotions	3
Other Administrative Actions	2
Counseling	4

### Summary of Investigations

<i>Classification of Investigations</i>	<i>Carryover</i>	<i>Opened Cases</i>	<i>Closed Cases</i>	<i>Cases In Progress</i>
A - Conflict of Interest	1	2	1	2
B - Internal Fraud	8	1	8	1
C - External Fraud	6	3	5	4
D - False Statements	2	2	4	0
E - Theft	1	2	1	2
F - Misuse of Government Property	12	9	18	3
G - Employee Misconduct	0	0	0	0
H - Management Misconduct	1	2	2	1
I - Technical Allegations — Other	9	11	12	8
J - Whistleblower Reprisal	1	0	1	0
Total Investigations	<u>41</u>	<u>32</u>	<u>52</u>	<u>21</u>
S - Event Inquiries	2	2	2	2
P -Special Projects	1	0	1	0



---

# OTHER ACTIVITIES

## **REGULATORY REVIEW**

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

The review encompasses issues raised in OIG investigations, audits, and prior regulatory commentaries. In examining submitted documents reflecting regulatory, statutory, and policy actions, the regulatory review program's main objective is to examine agency actions to assist in the elimination of fraud, waste, and abuse within the agency. In addition, comments are also used to address issues related to preserving OIG's independence and integrity under the office's statutory precept. Comments are made through formal memoranda as well as during meetings and discussions.

From April 1, 2003, through September 30, 2003, OIG reviewed 230 agency documents, including approximately 80 Commission papers (SECYs) and 150 Federal Register Notices, regulatory actions, and statutes.

During this period, several comments focused on management and process issues reflected in draft management directives. The most significant commentaries are summarized below.

During this period, several comments focused on draft MDs issued by the Division of Facilities and Security. Evidencing dedicated effort and focus, each of the draft directives provided guidance on updated organizational and functional changes resulting from the agency's enhanced efforts in security. OIG comments generally discussed the functional role of the Inspector General within the processes and procedures of the agency.

MD 12.1, "NRC Facility Security Program," generally provided comprehensive guidance and direction to agency employees. However, several matters related to OIG and other law enforcement authorities roles required more detail and clarification. Additional information was provided for inclusion in the directive on IG authority and statutory law enforcement authority. OIG also provided direction on the appropriate coordination with other Federal law enforcement agencies and authority for certain surveillance actions.

Specific OIG comments concerning MD 12.3, "NRC Personnel Security Program," addressed several critical issues. First was the need for a glossary to aid in understanding the myriad acronyms and terms of art used in security functions. In addition, OIG noted that MD 12.3 briefly discussed matters related to drug testing in the workplace. Because of the importance of this topic, OIG suggested that issues related to a "drug free workplace" and drug testing be addressed either in more depth within this directive or as a stand-alone directive. An additional specific comment was that further direction is necessary in the area of information technology access by contractors.

*(continued on next page)*

Another important concern regarding contractors identified in the directive is the need to deny access to contractor employees whose initial clearance review discloses issues, meaning information inconsistent with immediate clearance, until those issues are resolved. Finally, we suggested inclusion of a description of the IG position and authority along with a paragraph relating that IG investigative and audit findings relevant to security issues are provided to agency security officials, along with a statement that security information is provided to the OIG when necessary to conduct an investigation or audit.

Management Directive 12.5, “NRC Automated Information Security Program,” provides comprehensive direction on the complex and technical processes and procedures related to critical information security. Inclusion of the OIG and its role and functions in information technology security issues and actions was a repeated comment related in several topic areas of the directive. Another area of concern was the proper clearance of contractor employees for access to sensitive information technology. The OIG also provided guidance to further clarify appropriate coordination with other Federal law enforcement authorities and compliance with other Federal directives.

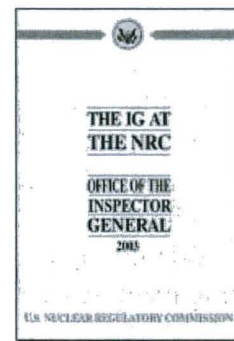
The Freedom of Information Act (FOIA) and Privacy Act provide a statutory foundation for critical information disclosure and protection in Federal agencies. Within NRC, dual responsibilities to keep the public informed while assuring protection of security and personal information make compliance with these statutes more complicated. Therefore, correct and clear guidance in the regulatory implementation of these statutes is essential. In furtherance of the objective to assure compliance, the agency convened a FOIA review group, drafted revisions to Part 9 of Title 10 of the Code of Federal Regulations, and updated MD 3.2, “Privacy Act.”

OIG remarks to the review group focused on OIG cognizance over documents and information within its organizational responsibility. Agreement was reached regarding policies and procedures appropriate to adequately protect sensitive OIG documents. Similarly, OIG comments on revision to MD 3.2 reflected that OIG ongoing communication provided mutual understanding and agreement which were correctly conveyed in the well written and comprehensive update to the directive.

Comments on the proposed rule to amend 10 Code of Federal Regulations, Part 9, Subparts A and B, focused primarily on concerns related to the efficient processing of FOIA and Privacy Act within the OIG domain. Particular concern and attention was directed to assuring protection of OIG documents.

## **THE IG AT THE NRC**

The 4<sup>th</sup> Edition of “The IG at the NRC” was published in September 2003. This publication serves as the primary reference for the organizational structure and functions, policies, procedures, and legal authorities relevant to the OIG mission. Highlights of this edition include an explanation of the new statutory law enforcement authority and a description of revised audit procedures. In addition, more detailed guidance is provided on the OIG Hotline, including the availability of electronic reporting and requests for OIG documents under the FOIA. This volume was distributed to all agency employees and published on the OIG Web site.



## **TRAINING AT THE INSPECTORS GENERAL INSTITUTE**

On May 14, 2003, the General Counsel to the NRC Inspector General and the Deputy Counsel to the Environmental Protection Agency Inspector General taught at the Inspectors General Institute at its conference in Chicago. The class was part of a week-long seminar for Federal, State, and municipal Inspectors General. In addition to preparing the text syllabus for the legal issues segment of the course, they developed and led the class in discussion and exercises. Course topics included major Federal fraud statutes, criminal and civil prosecution processes, attorney-client privilege, and jurisdiction. The presentation focused on aspects of these legal areas most relevant to the functions of Inspectors General. Case examples were used to illustrate points including sensitive matters of wrongdoing by public officials and cooperation between different agencies. The exercise problems provided an opportunity for seminar attendees to apply the legal concepts to factual situations and present their analyses and conclusions.

## **NRC OIG TACTICAL TRAINING FACILITY**

Section 6(e)(4) of the Inspector General Act of 1978, as amended in 2002, governs the exercise of law enforcement authorities for those Inspector General offices that have been granted statutory law enforcement authorities. With enactment of Section 6(e) of the IG Act, the Attorney General, after an initial determination of need, may authorize law enforcement powers for eligible personnel of each of the various offices of presidentially appointed Inspectors General. These special law enforcement powers may only be authorized



*Computer Forensics Laboratory at the NRC OIG Technical Training Facility*

after each IG office meets certain prerequisites. Each year the IG offices must certify that each criminal investigator has completed the Basic Criminal Investigator Training Program, firearms training, and qualifications requirements, and that they abide by the deadly force policy established by the Department of Justice (DOJ).

The NRC Office of the Inspector General (OIG) Technical Training Facility (TTF) was established and houses all training equipment, the evidence repository, the technical operations support equipment, and the Computer Crimes Unit, including the computer forensics laboratory. One important aspect of the TTF is the annual judgment pistol shooting conducted with the simulated Firearms Training System. The NRC OIG firearms instructor certifies twice each year that every criminal investigator has completed this judgment pistol shooting training and is competent and knowledgeable of DOJ's deadly force policy. Another important aspect

*(continued on next page)*

of the training performed at the TTF is defensive measures training, which includes self-defense techniques and baton training.

The TTF is used for training not only NRC OIG criminal investigators, but other Federal law enforcement employees as well. Many agencies have either trained or requested use of the NRC TTF. These agencies include OIGs from the General Services Administration, Department of Health & Human Services,

Social Security Administration, Department of Energy, and Department of Education, as well as law enforcement personnel from the Federal Bureau of Investigation, the Food & Drug Administration, and NRC's Office of Investigations. NRC OIG and its TTF have received the appreciation of many of these offices for not only sharing this training facility but also for providing valuable technical support and instruction.

---

# APPENDICES

---

## **AUDIT LISTINGS**

---

### *Internal Program Audit and Special Evaluation Reports*

<b>Date</b>	<b>Title</b>	<b>Audit Number</b>
04/21/03	Computer Security Review of Region I - King of Prussia, Pennsylvania	OIG- 03-A-13
05/13/03	Computer Security Review of Region III - Lisle, Illinois	OIG-03-A-14
05/26/03	Audit of NRC's Regulatory Oversight of Special Nuclear Materials	OIG-03-A-15
06/05/03	NRC's Oversight of Research and Test Reactors	OIG-03-A-16
06/09/03	Memorandum Report: Review of NRC's Purchase Order Processing	OIG-03-A-17
06/13/03	Computer Security Review of Region II - Atlanta, Georgia	OIG-03-A-18
07/09/03	Independent Auditor's Report: Closeout of Audit of GSE Power Systems, Inc.	OIG-03-A-19
07/23/03	Computer Security Review of Region IV - Arlington, Texas	OIG-03-A-20
09/02/03	Memorandum Report: Follow-up Review of NRC's Internet Usage	OIG-03-A-21
09/12/03	Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for FY 2003	OIG-03-A-22

---

**Contract Audit Reports**

---

<b>OIG Issue Date</b>	<b>Contractor/ Contract Number</b>	<b>Questioned Costs</b>	<b>Unsupported Costs</b>
04/23/03	Sciencetech, Inc. NRC-02-98-001	0	0
	NRC-03-95-026	0	0
	NRC-04-94-045	0	0
	NRC-04-96-041	0	0
	NRC-04-96-060	0	0
	NRC-04-97-039	0	0
	NRC-08-97-302	0	0
	NRC-26-00-300	0	0
	NRC-26-95-261	0	0
06/03/03	Information Systems Laboratories, Inc. (ISL) RFP-NRR-03-038	0	0
06/12/03	Empyrean Services, LLC RFP-NRR-03-038		
06/13/03	GSE Power Systems, Inc. NRC-26-96-265	\$ 97,758	0
07/10/03	Engineering Mechanics Corporation RS-RES-03-046	0	0
07/31/03	Beckman and Associates, Inc. NRC-03-98-021	\$107,638	0
09/04/03	Applied Programming Technology, Inc. RS-RES-03-057	0	0
09/30/03	Athey Consulting, Inc. NRC-26-98-262	0	0

## AUDIT TABLES

During this reporting period, OIG analyzed seven contract audit reports issued by the DCAA and one audit report issued by an independent accounting firm.

**Table I. Post-Award Findings**

<b>OIG Reports Containing Questioned Costs April 1, 2003 – September 30, 2003</b>			
<b>Reports</b>	<b>Number of Reports</b>	<b>Questioned Costs (Dollars)</b>	<b>Unsupported Costs (Dollars)</b>
A. For which no management decision had been made by the commencement of the reporting period	1	\$38,433*	\$3,606,365*
B. Which were issued during the reporting period	2	205,396	0
<i>Subtotal (A + B)</i>	2	205,396	0
C. For which a management decision was made during the reporting period:			
(i) dollar value of disallowed costs	2	205,396	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	0	0	0
E. For which no management decision was made within 6 months of issuance	1	\$38,433*	\$3,606,365*

\* 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. Pre-Award Findings**

---

**OIG Reports Issued with Recommendations  
That Funds Be Put to Better Use  
April 1, 2003 – September 30, 2003**

---

<b>Reports</b>	<b>Number of Reports</b>	<b>Dollar Value of Funds</b>
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	0	0
<i>Subtotal (A + B)</i>	0	0
C. For which a management decision was made during the reporting period:		
(i) dollar value of recommendations that were agreed to by management	0	0
(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



---

## **ABBREVIATIONS**

DBD	design basis document
DCAA	U.S. Defense Contract Audit Agency
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DSR	Discontinued Service Retirement
ECIE	Executive Council on Integrity & Efficiency
EI	Event Inquiry
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GC	General Counsel (OIG)
GSA	U.S. General Services Administration
GSS	General Support System
HEW	U.S. Department of Health, Education, and Welfare
IG	Inspector General
IP2	Indian Point Unit 2 Power Plant
IT	information technology
MA	Major Applications
MC&A	Material Control and Accountability
MD	Management Directive
NIST	National Institute of Standards and Technology
NMMSS	Nuclear Materials Management and Safeguards System
NRC	U.S. Nuclear Regulatory Commission
OIG	Office of the Inspector General (NRC)
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
PCIE	President's Council on Integrity & Efficiency
RMOS	Resource Management and Operations Support (NRC OIG)
RPS	reactor protection system
RPV	reactor pressure vessel
SNM	special nuclear material
TTF	Technical Training Facility (NRC/OIG)
UFSAR	Updated Final Safety Analysis Report

---

## REPORTING REQUIREMENTS INDEX

*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.*

<b>CITATION</b>	<b>REPORTING REQUIREMENTS</b>	<b>PAGE</b>
Section 4(a)(2)	Review of Legislation and Regulations .....	23
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies .....	9-12,17-20
Section 5(a)(2)	Recommendations for Corrective Action .....	9-12
Section 5(a)(3)	Prior Significant Recommendations Not Yet Completed .....	None
Section 5(a)(4)	Matters Referred to Prosecutive Authorities .....	18
Section 5(a)(5)	Information or Assistance Refused .....	None
Section 5(a)(6)	Listing of Audit Reports .....	27
Section 5(a)(7)	Summary of Significant Reports .....	9-12, 17-20
Section 5(a)(8)	Audit Reports — Questioned Costs .....	29
Section 5(a)(9)	Audit Reports — Funds Put to Better Use .....	30
Section 5(a)(10)	Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made .....	None
Section 5(a)(11)	Significant Revised Management Decisions .....	None
Section 5(a)(12)	Significant Management Decisions With Which the OIG Disagreed .....	None

## THE NRC OIG HOTLINE

The Office of the Inspector General at NRC established the Hotline Program to provide NRC employees, other Government employees, licensee/utility employees, contractors and the public with a confidential means of reporting suspicious activity to the OIG concerning fraud, waste, abuse, employee or management misconduct. Mismanagement of agency programs or danger to public health and safety may also be reported through the Hotline.

We do not attempt to identify persons contacting the Hotline. Persons may contact the OIG by telephone, through an on-line form, via the NRC public Web site [www.nrc.gov](http://www.nrc.gov) or by mail. There is no caller identification feature associated with the Hotline or any other telephone line in the Inspector General's office. No identifying information is captured when you submit an on-line form. You may provide your name, address, or phone number, if you wish.

### 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

**Call:**           **OIG Hotline**  
**1-800-233-3497**  
9:00 a.m. - 4:00 p.m. (EST)  
After hours, please leave a message

**Submit:**       On-Line Form  
Access by: logging onto [www.nrc.gov](http://www.nrc.gov)  
Click on Inspector General  
Click on OIG Hotline phone symbol

or **Write:**      U.S. Nuclear Regulatory Commission  
Office of the Inspector General  
Hotline Program  
Mail Stop T-5 D28  
11545 Rockville Pike  
Rockville, MD 20852-2738

