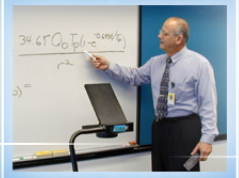






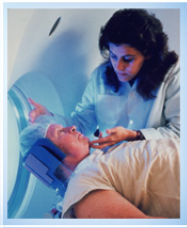



The NRC OIG: Who We Are and What We Do

Beth Serepca

3/20/06



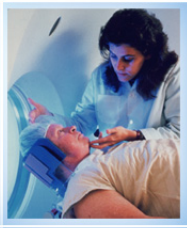


The Agency

- The Energy Reorganization Act of 1974 established the independent U.S. Nuclear Regulatory Commission to regulate commercial uses of nuclear material; other duties of the former Atomic Energy Commission were assigned to the Department of Energy.

- The NRC is headed by four Commissioners and a Chairman, all appointed by the President and confirmed by the Senate for staggered five-year terms. No more than three can be from the same political party.

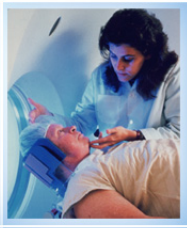




The Agency

- The NRC employs about 3,000 people in its suburban Maryland headquarters and four regional offices in Pennsylvania, Georgia, Illinois and Texas.

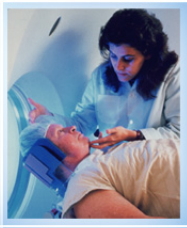




The NRC Regulates:

- Nuclear reactors - commercial power reactors, research and test reactors, new reactor designs;
- Nuclear materials - nuclear reactor fuel, radioactive materials for medical, industrial and academic use;
- Nuclear waste – transportation, storage and disposal of nuclear material and waste, decommissioning of nuclear facilities; and
- Nuclear security – physical security of nuclear facilities and materials from sabotage or attacks.

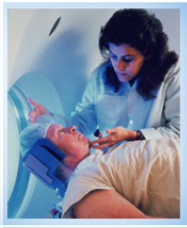




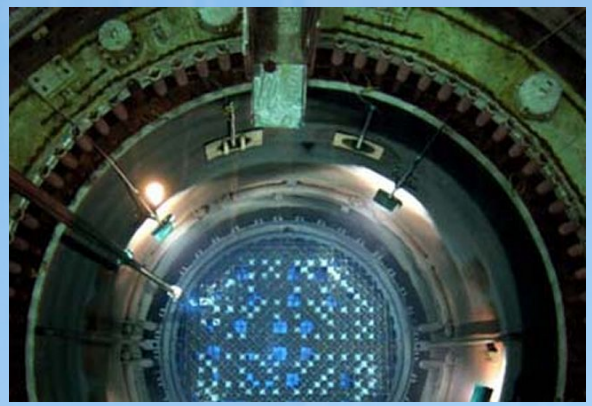
What the Agency doesn't do:

- Regulate nuclear weapons, military reactors or space vehicle reactors. (These are regulated by other federal agencies.)
- Own or operate nuclear power plants.
- Regulate some radioactive materials, such as naturally occurring radon, X-rays and material produced in particle accelerators. (These are regulated by states or other federal agencies.)





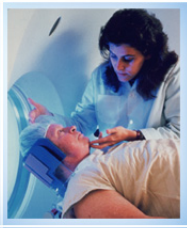
NRC Computer Security Resources



Formal program since 1980

Senior Information Technology Security Officer established in 2001

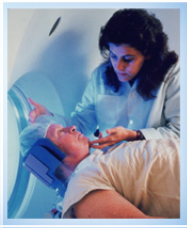




NRC Computer Security Program Guidance

- Management Directives
- Mandatory Training
- Network Announcements



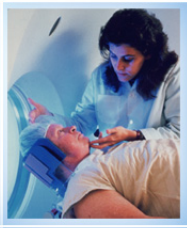


NRC's FISMA Implementation

Inventory and classify all systems as:

- MA
- GSS
- Listed systems
- Other



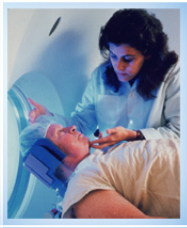


NRC Computer Security Program Implementation

Capture and track all findings from:

Risk Assessments
System Security Plan
Security Test and Evaluation
Contingency Plan Testing
Certification and Accreditation

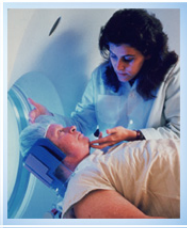




NRC Computer Security Program

- Track Plan of Action and Milestones
- Approval to operate provided after security issues resolved
- All security documentation reviewed and updated
- Security Awareness course on-line





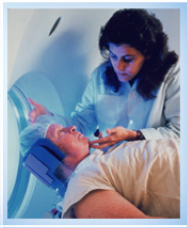
OIG

Audits and Investigations

- Audits – 3 teams
  - Follow audit principles
  - Internal Audit Definition – Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

- Investigations – 2 teams
  - Follow Federal investigation standards

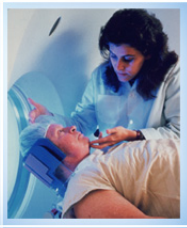




FISMA Audits

- Approach is to audit throughout the year
- There are about 30 systems in operation

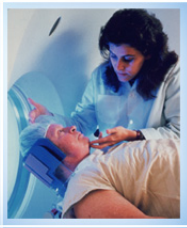




FISMA Audits Completed in 2005

- Independent Evaluation of FISMA
- Evaluation of NRC's Certification and Accreditation Efforts
- Evaluation of NRC's Automated Information System Inventory Process
- Evaluation of Listed Systems that Process Safeguards and/or Classified Information
- System Evaluation of Security Control for Standalone Personal Computers and Laptops



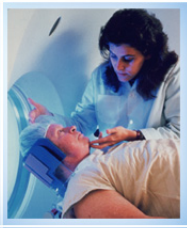


Additional Audit Efforts to Support FISMA

- Regional computer security audits
- Determine adequacy of the region's information security program and practices

- 5 Areas Reviewed
  - Physical access controls
  - Logical access controls
  - Configuration management
  - Security program
  - Continuity of operations

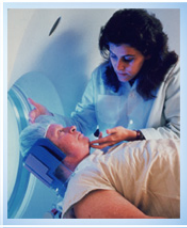




More Areas Under FISMA

- More information security areas are being included such as compliance with the Privacy Act and E-Authentication
- How do you feel about that?





Contact Information

Beth H Serepca

Team Leader, Security and
Information Management Team

US Nuclear Regulatory Commission

Office of the Inspector General

(301)415-5911

BHS@NRC.GOV