Strengthening FISMA Capabilities by Building on successful IT Reviews: an OIG Perspective on Risk Management and Awareness Through Education

Beth Serepca

FISSEA Conference,
March 25, 2009

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Risk Management Definition

- A basic principle of risk management is to determine the greatest sources of threats and vulnerabilities.

Risk Management

The agency manages risk and so does the OIG

OIG Risk

OIG conducts audits in areas that are the most vulnerable to waste, fraud and abuse.

NRC OIG Audit Areas

- To select our audit areas we fill out a risk assessment questionnaire on every potential area we are thinking of reviewing. The ones with the most risk significant scores are the ones we put into our audit plan.

Mandatory Audits

- We also conduct the mandatory audits such as FISMA. These are automatically given a 100 percent risk score in our questionnaires.

FISMA

- FISMA focuses on process, not technology. It needs to shift to a more operational focus on risk management.

FISMA

- So has FISMA made us more secure?
- We measure compliance but FISMA helps in managing IT risk in a systematic, repeatable way.

FISMA

- FISMA has laid out the groundwork for building a systematic process for managing risk and improving security.

FISMA

- We conduct FISMA audits at HQ and at the 4 NRC regional offices.
- We look for credible risks.
- Regions will be reviewed in 2009.

FISMA

- We also perform information security audits during the year
- Examples - Laptop audit and NSTS

Information Security Audits

- What We Found

Agency IT Alignment

- NRC aligns IT with business strategies. NRC manages IT spending to NRC's core business.

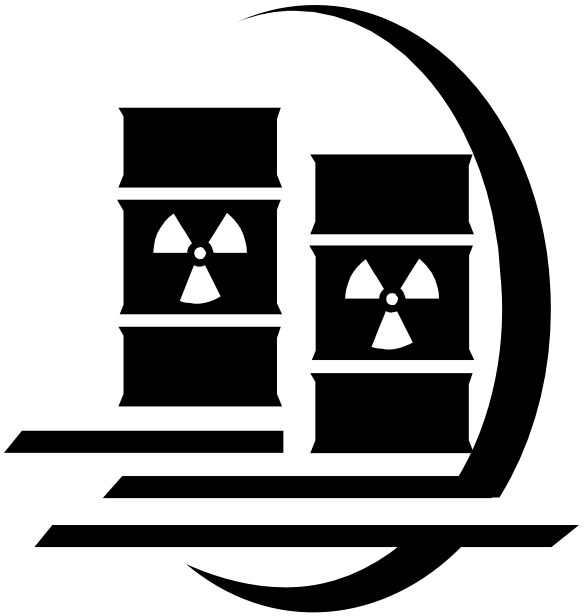
- Mission is to protect public health and safety and the environment

September 11, 2001

- NRC shifted its IT spending priorities to align with keeping radioactive material out of terrorist hands.

EPA of 2005

- The EPA of 2005 required NRC to issue regulations establishing a mandatory tracking system for radiation sources.



National Source Tracking System

- System is the first system to be implemented as a high system for CIA
- 15 million contract
- Over 3 years to develop and implement

National Source Tracking System

- Companies will use NSTS to report how much radioactive material is in inventory

National Source Tracking System

- Access will be limited and controlled by an NRC issued digital certificate on a separate hard token

OIG Findings

We found that:

- Delays increased contract costs, postponed development by 18 months and we raised questions about future IT systems

Contact Information

- Beth Serepca, NRC OIG, Team Leader