



**U.S. NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **Cyber Security**

Catherine Haney, Director  
Office of Nuclear Material Safety and Safeguards  
U.S. Nuclear Regulatory Commission  
May 30, 2013

# Overview

- Cyber Threat
- NRC Considerations
- NRC Cyber Security Roadmap
- Where We Are Today
- Key Messages

# Cyber Threat

- The Cyber Threat Landscape is Dynamic and Evolving
- Cyber Attacks Part of the Design Basis Threat (DBT)
- Types of Cyber Threats:
  - Outsider
  - Insider
  - Supply Chain

# NRC Considerations

- Safety – radiological sabotage, including chemical exposures and criticalities
- Physical Security – theft and diversion of material
- Information Security – loss of classified information and materials
- Materials Control & Accountability – theft and diversion of materials
- Emergency Preparedness – impacts to public health and safety in the event of an emergency

# Cyber Security Roadmap

- SECY 12-0088, June 25, 2012
- Provides an update on the status of the implementation of cyber security requirements for power reactor licensees and Combined License applicants
- The Roadmap outlines the approach for evaluating the need for cyber security requirements for the following four categories of the NRC licensees and facilities:
  - Fuel cycle facilities
  - Non-power reactors
  - Independent Spent Fuel Storage Installations
  - Byproduct materials licensees

# Where We Are Today

- Escalating Importance of Cyber Security
- National and International Efforts
- Impact on NRC Programs
- Not All Licensees Are the Same
- Lessons Learned from Power Reactors
  - Programmatic, Performance-Based Approach
  - Reliance on Standards and Best Practices
  - Importance of Governance Strategies
  - Cyber Security is a Process vs. Task

# Key Messages

- Shaping the Regulatory Landscape for the Future
- Senior Management Engagement
- Workforce Development

# Questions

