Department of Energy
2008-2014 Graded Security
Protection (GSP) Policy
February 2014
Graded Security Protection Policy

- Explicitly implements concepts intended to ensure a balanced risk management foundation for security system planning in a resource-sensitive environment
  - Informed by National Intelligence threat capabilities assessments (Likelihood)
  - Aligns Departmental assets into one of five Security Protection Levels (Consequence)
Graded Security Protection Policy

• Information regarding likelihood and consequence are melded with baseline Departmental requirements to delineate performance metrics for protection of:
  – Nuclear weapons
  – Nuclear weapon components
  – SNM
  – Other Departmental assets
Graded Security Protection Policy

• Provides adversary types, numbers, and capabilities for each SPL
• Establishes the requirement for vulnerability analyses and risk assessments depending on SPL
• Defines the methodology for determining the effectiveness of the physical protection program
• Establishes a framework for a formal peer review of scenarios used in an analysis
2014 Revision

- Updated to include lessons learned from national events and DOE/NNSA incidents
- Clarify Departmental expectations
- Implements a new requirements to conduct risk assessments at all DOE facilities
- Requires DOE facilities to implement measures to address an active shooter scenario
Summary

• The GSP policy revision:
  – Implements risk-informed concepts and principles
  – Provides better direction and understanding of the policy’s intent
  – Realigns the adversary based planning metrics to ensure it reflects a rational and representative terrorist threat
  – Provides more credible performance thresholds for ensuring a more prudent expenditure of resources
  – Incorporates lessons learned from recent real world events