

---

# ABA Section of Public Utility, Communications & Transportation Law

*Safety and Security in Transport*

## Commercial Nuclear Power Plants

---

Stan Blanton

Nuclear Power Subcommittee



BALCH & BINGHAM LLP

Alabama • Georgia • Mississippi • Washington, D.C.

---

# The Regulatory Landscape

- NRC Security Regulations Before & After 9/11 Cover:
  - ❑ restricted data
  - ❑ national security information
  - ❑ classified information
  - ❑ storage of special nuclear material
  - ❑ transport of special nuclear material
  - ❑ physical security of facilities
  - ❑ safeguards on nuclear material
  - ❑ employment clearance

---

# The Regulatory Landscape

- Pre-9/11: Comprehensive Security Regulations
- Physical Protection
  - Written Security Plan
  - Access Control
    - Background checks for employees
    - Safeguards access control
    - Limited physical access to the facility
  - Vehicle Barrier Systems
  - Armed Security Forces
    - Force-on-force drilling
    - Graded performance
  - Safeguards

---

# Pre 9/11: Key Areas of Focus

## ■ PHYSICAL

- Responding to traditional external threats
  - Less expansive Design Basis Threat
  - “Enemies of the state” distinction
- Protection during facility operation

## ■ INFORMATION

- Responding to traditional external threats
  - Safeguards information
  - Little focus on cyber security

Protection from Internal Threats:  
Screening for Physical and Information  
Access

---

# Post 9/11 Regulatory Process

- Major Orders
    - February 2002 Orders - increased patrols, augmented security forces and capabilities, additional security posts & physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, more restrictive site access controls
    - 2002-2003 Orders - enhancements from other facilities (e.g. decommissioning facilities and enrichment facilities)
    - April 2003 Orders - work hours, training, and qualification requirements for security personnel
  - Major Rulemakings
    - January 2007 – Final Rule revising Design Basis Threat Regulations
    - October 2008 – Final Rule revising Protection of Safeguards Information Regulations
    - March 2009 – Final Rule revising Power Reactor Security Requirements
    - June 2009 – Final Aircraft Impact Rule
-

---

## Post 9/11: Key Areas of Enhancement

- Revised Design Basis Threat Regulations
- Greater Protection of Spent Fuel Pool
- Intensified Protection of Safeguards Information
- Additional Cyber-security
- Enhanced Access Control
- New Aircraft Impact Rule
- Intensified Construction Security

---

# Post 9/11: Key Areas of Enhancement

## ■ PHYSICAL

- Responding to new external threats
  - Aircraft
  - Spent fuel pool

## ■ INFORMATION

- Responding to new external threats
  - Safeguards information
  - Cyber-security

Protection from Internal Threats:  
Enhanced Screening for Physical and  
Information Access

---

# Facility Physical Security Plan

- Design Basis Threat (DBT): “general adversary characteristics that designated licensees must defend against with high assurance”
  - Design Features
  - Defensive Forces
- Post 9/11 orders: protect from more types of attacks
- 2005 Energy Policy Act requires DBT revision
- March 2007 – Final Rule revising the DBT (mostly incorporates earlier orders)
- Continuing periodic threat reviews

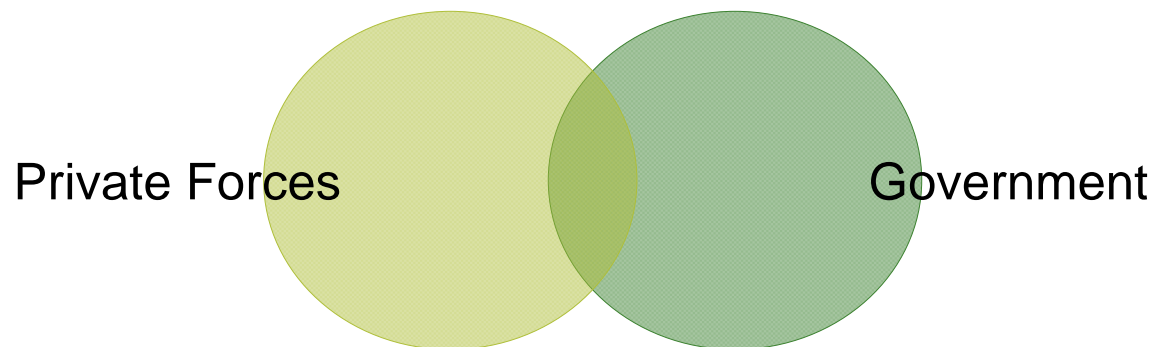
---

# Facility Physical Security Plan: DBT

- The Adversary: Armed, military training, kill-or-be-killed mentality, knowledge of target
  - May include assistance from inside individual(s)
- The Method: Land- or water-borne vehicle bomb, maybe with external assault; one or more points of entry by one or more individuals
  - By stealth or otherwise
  - May coordinate with cyber attack
- The Goal: Radiological sabotage or theft of strategic special nuclear material

# Facility Physical Security: Final DBT Rule

- “In the Commission’s view, establishing set boundaries demarcating [between the licensee and the government] is neither possible nor desirable.”
- DBT only covers threats “a private security force can reasonably be expected to defend” against



***Aircraft attack is a “beyond-DBT event”***

***Licensees do not have to protect against aircraft attack***

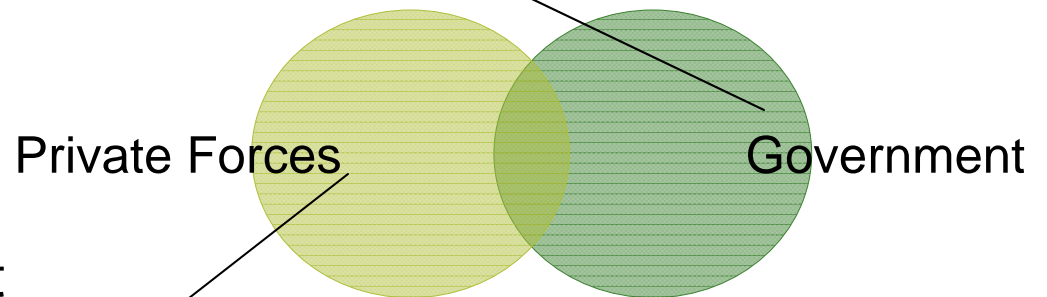
# Facility Physical Security: Division of Responsibility

## ■ Government's Realm:

- Protection from Aircraft Assault
- Protection from Missiles
- U.S. Defense Activities

## ■ Private Realm:

- Adversaries and vehicles/equipment that can be actively engaged
- Defenses not requiring military weapons or law enforcement authority



---

# What provisions do exist to protect from an airplane attack, like 9/11?

- Aircraft Impact Rule
    - Aircraft Impact Assessment – new plants must consider in their application how an impact would affect key safety functions
      - Intends reduced use of operator action
      - Design features
        - plant containment
        - core cooling capability
        - spent fuel pool remain intact
    - If current design does not allow these key functions after an impact, applicant must consider other design options
  - Licensee plans to contain/mitigate effects of aircraft impact
  - Existing nuclear facilities' robust design features
-



*Hur hållbara är kraftstationerna, då?  
Här är ett nytt test med ett F4 plan.*

**COMPFUSED.COM**

---

# NEPA Consideration of Terror Attacks

## **NRC Position – no consideration of terror attacks in NEPA review because:**

- Too far removed
- Risk cannot be determined
- NEPA does not require “worst case” analysis
- Public process not appropriate forum for sensitive security issues.

## **CIRCUIT SPLIT**

**9th Circuit, 2006 (new facility license):** NRC Position unreasonable because NRC otherwise considered attacks

**3d Circuit, 2009 (relicensing):** NRC Position reasonable because no “reasonably close causal relationship”

# Facility Physical Security Plan: Spent Fuel

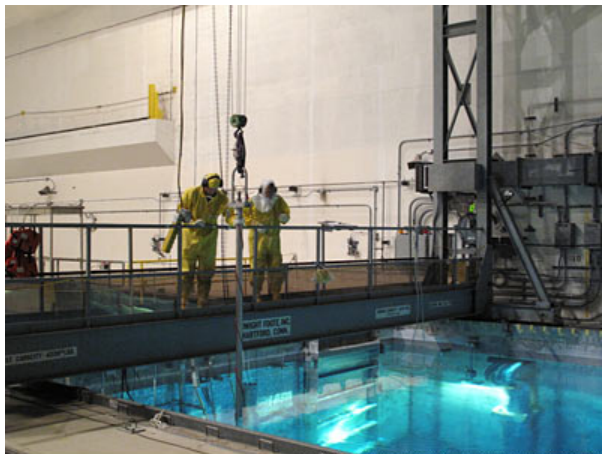
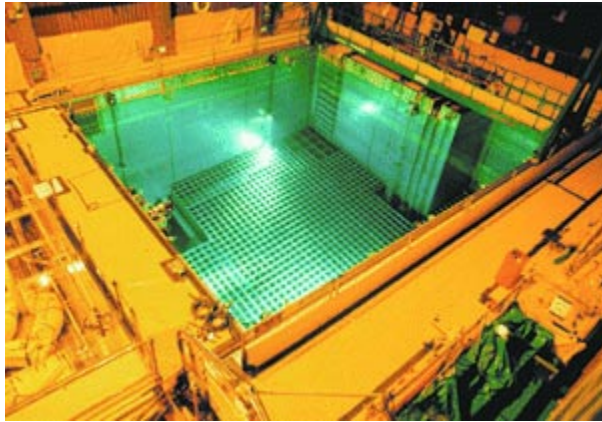


PHOTO: STEVE HARGREAVES/CNNMONEY.COM

- Key Security Features:
  - ❑ Stored only within Protected Area
  - ❑ Intrusion detection (including methods to identify false alarms)
  - ❑ Response to intrusions
  - ❑ Assistance from Local, State, and Federal agencies
  - ❑ Allow access only to authorized employees

---

# Transportation of Special Nuclear Material

- In-transit physical protection system must:
    - Restrict access/activity near transports
      - Pre-plan itineraries
      - Knowledge of route conditions & SNM's status and position en route
      - Determine alternative itineraries en route when warranted
    - Detect/delay attacks by force, stealth, or deceit
      - Access authorization (current authorization schedules, entry criteria)
      - Verify identity of persons & materials
      - Inspection & detection procedures for unauthorized tampering with transports/containers
      - Surveillance
  - Security Personnel Require:
    - Equipment, vehicle design features, & procedures for protection
    - Adequate communications systems
    - Predetermined plan to respond to contingency events
    - Liaisons with local law enforcement for assistance en route
-

---

# Information Security:

## Safeguards Information

- Info not classified as National Security Information or Restricted Data
- Licensee's/applicant's detailed control & accounting procedures for physical protection of special nuclear material
- Detailed security measures for the physical protection of source, byproduct, or special nuclear material including:
  - Security plans
  - Procedures
  - Equipment

---

# Information Security: Safeguards Information

- Requires “need to know” clearance
  - Applies to NRC info also, for example:
    - specifics of the DBT regulations
    - assumptions like type of aircraft, speed, angle of impact for Aircraft Impact Rule
- An information protection system (“stand-alone,” non-networked computer)
- Supervised by cleared individual or under lock & key with access only by same
- Every SGI document must be marked

---

# Information Security: Cyber Security

- Protection must include “up to and including” DBTs
  - Cyber Security Plan is required, including protection:
    - related to safety, security or emergency preparedness
    - from attacks that would compromise confidential data, access to data, or system operations
  - Licensee must:
    - analyze systems & networks; identify assets to be protected
    - establish, implement, & maintain a Cyber Security Program
    - apply & maintain “defensive in-depth protective strategies” to ensure
      - Detection (timeliness)
      - Response
      - Recovery (“correct exploited vulnerabilities”)
      - Effects are mitigated
    - train personnel to perform necessary tasks
-

---

# Information Security: Cyber Security

March 2009: FERC Order 706-B

- Attempts to fill “regulatory gap”
- CIP Standards – Critical Infrastructure
- NRC Regulations – Safety Related SSCs

January 2010: NRC – NERC MOU regarding NRC cyber security regulations and Reliability and CIP Standards

## ■ FERC: Jurisdiction over transmission lines

- Any “balance of plant equipment” not regulated by NRC is covered by FERC (Order 706-B)
- NERC required nuclear facilities to comply with their CIP
- March 2010: FERC delays compliance because no bright-line jurisdictional distinction

## ■ NRC: Jurisdiction over nuclear facilities

- Cyber Security regulations do not cover all equipment in plant that might affect the grid’s reliability (Example: excludes power continuity systems)
- Currently, still a lack of specific items NRC wants exempted from FERC’s regulation

---

# Controlling Access

- Screening Required For:
  - Facility Employees
    - Depends on particular facility access (Protected Area? Security Force?)
  - Construction Employees
  - Information Access
- The Screening Process: “Access Authorization Program”
  - Credit, background, and criminal checks
  - Unescorted access
  - Must be requested from NRC for those seeking access to classified information
  - Safeguards Information requires “need to know” clearance
  - Preliminary Construction Security Rule – more stringent screening for construction employees (demographic checks, fingerprinting)

---

# Controlling Access

- Continued Oversight of Personnel
  - “Fitness for Duty Program” requires testing and reporting for behavior that could affect safety or security, including:
    - Drug or alcohol abuse
    - Arrests, indictments, court-mandated drug or alcohol recovery program
  - “Behavioral Observation Program” requires employees to spot evidence of such behavior, including:
    - Drug or alcohol abuse
    - Illness
    - Behavioral changes
    - “Aberrant” behavior

---

# Construction Security

- “Access Authorization and Physical Security for Nuclear Power Plant Construction”
  - Construction security plan “to provide assurance that malicious acts during construction cannot later reasonably result directly or indirectly in radiological sabotage”
  - 4 Phases:
    - 1) Structural concrete:
      - background checks
      - behavioral observation program
      - security patrols
      - construction site security force
    - 2) Onsite in-place security or safety-related SSCs:
      - additional access control
      - vehicle/person search requirements
    - 3) Transition to the physical security plan:
      - security sweeps
      - lockdown of controlled access construction areas
      - barriers to unauthorized penetration attempts
      - surveillance and monitoring
    - 4) Phase 4 - Licensee discontinues requirements of this section in favor of its operational security program
-

---

Questions?

---