Group D

FOIA/PA NO: 2013-0062

RECORDS BEING RELEASED IN PART

The following types of information are being withheld:

Ex. 1: ☐ Records properly classified pursuant to Executive Order 13526
Ex. 2: ☐ Records regarding personnel rules and/or human capital administration
Ex. 3: ☐ Information about the design, manufacture, or utilization of nuclear weapons
☐ Information about the protection or security of reactors and nuclear materials
☐ Contractor proposals not incorporated into a final contract with the NRC
☐ Other_____
Ex. 4: ☐ Proprietary information provided by a submitter to the NRC
☐ Other_____
Ex. 5: ☐ Draft documents or other pre-decisional deliberative documents (D.P. Privilege)
☐ Records prepared by counsel in anticipation of litigation (A.W.P. Privilege)
☐ Privileged communications between counsel and a client (A.C. Privilege)
☐ Other_____
Ex. 6: ☑ Agency employee PII, including SSN, contact information, birthdates, etc.
☐ Third party PII, including names, phone numbers, or other personal information
Ex. 7(A): ☐ Copies of ongoing investigation case files, exhibits, notes, ROI's, etc.
☐ Records that reference or are related to a separate ongoing investigation(s)
Ex. 7(C): ☐ Special Agent or other law enforcement PII
☐ PII of third parties referenced in records compiled for law enforcement purposes
Ex. 7(D): ☐ Witnesses' and Allegers' PII in law enforcement records
☐ Confidential Informant or law enforcement information provided by other entity
Ex. 7(E): ☐ Law Enforcement Technique/Procedure used for criminal investigations
☐ Technique or procedure used for security or prevention of criminal activity
Ex. 7(F): ☑ Information that could aid a terrorist or compromise security

Other/Comments:_____

Sexton, Kimberly

From: Sexton, Kimberly
Sent: Friday, December 07, 2012 5:29 PM
To: 'ZORN, Jason'
Subject: RE: FYI: letter

Hi there,

I'm clued in to this tangentially. I know Andrea is following (but I don't how closely). I'll take a look at this though.

Kimberly

From: ZORN, Jason [mailto:jcz@nei.org]
Sent: Thursday, December 06, 2012 8:26 AM
To: Sexton, Kimberly
Subject: FW: FYI: letter

FYI. I'm not sure if you are plugged into this, but as you scan see from the recent attached letter, the staff has plans to develop and issue orders to fuel cycle facilities regarding cyber security. This despite the fact that there is no clear understanding of the scope of what such a requirement would cover for those facilities, what the performance basis would be for such requirement (reactors at least have "radiological sabotage"), and the fact that the Commission seems rightfully focused on ensuring that new regulatory initiatives are subject to a comprehensive regulatory basis development whereby stakeholders can scrutinize and have an adequate opportunity to comment on proposed new requirements. Instead, the staff seems to be pursuing an order (11 years notably after 9/11) that will provide no transparency, no regulatory basis development, and virtually no stakeholder interaction. More examples of the staff trying to take the "fast and easy" approach because they find the appropriate processes – i.e. rulemaking -- too slow and too difficult. Just passing that along.

Jason

From: MAUER, Andrew
Sent: Wednesday, December 05, 2012 4:42 PM
To: ZORN, Jason
Subject: Fwd: FYI: letter

Begin forwarded message:

> **From:** "Smith, Brian" <Brian.Smith@nrc.gov>
> **Date:** December 5, 2012, 1:09:54 PM EST
> **To:** "MAUER, Andrew" <anm@nei.org>
> **Subject: FYI: letter**
>
> Electronic copy of what you have.
>
> I would plan on no more than 8 attending from NRC at the meeting. I invited John, Trish, and Christiana; not sure if they will attend.
>
> Brian

November 27, 2012

Mr. Andrew N. Mauer
Senior Project Manager
Fuel & Materials Safety
Nuclear Generation Division
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708

SUBJECT: RESPONSE TO JULY 10, 2012, LETTER ON CYBER SECURITY FOR FUEL CYCLE FACILITIES

Dear Mr. Mauer:

The U.S. Nuclear Regulatory Commission (NRC) appreciates the comments and proposal outlined in the Nuclear Energy Institute's (NEI's) July 10, 2012, letter regarding the NRC's actions on fuel cycle cyber security. Our discussions have identified two options (licensee initiative or NRC order) to accomplish the initial actions considered by the NRC staff to be of near term safety and security importance.

In your letter, a proposed path forward of the licensee initiative involves formation of an industry working group to develop guidance on four of the initial actions of importance and then, 120 days later, discuss the preferred strategy for implementation (voluntary license commitment or NRC order). Additionally, your letter suggests that if the NRC's focus is only on (b)(7)(F) (b)(7)(F) industry would also be willing to develop guidance on the other two initial actions of importance.

The NRC staff is concerned that your proposal would take longer and be less successful than anticipated, given the lack of industry consensus. The lack of consensus is highlighted by the July 23, 2012, letter received by the NRC from Babcock & Wilcox Nuclear Operations Group and statements by other licensees at the 2012 Fuel Cycle Information Exchange. Furthermore,

(b)(7)(F)

To more expeditiously and definitively address the identified safety and security concerns, the NRC staff is planning to draft orders specifying the actions of near term importance. It is the NRC staff's intent to provide the industry with the opportunity to comment on the draft requirements and to be involved with the development of the corresponding guidance document. The NRC staff is currently preparing a Commission paper which seeks permission to issue orders and proceed with the intended rulemaking.

The NRC staff also acknowledges the lack of understanding expressed by licensees concerning the cyber security threat. A cyber security "threat conference" is currently being planned to have both government and private sector experts better inform licensees of current cyber threats and risks. More information, discussion, and coordination of this conference can be expected within the next few months.

If you have any questions, I can be reached at 301-492-3137, or via e-mail at brian.smith@nrc.gov.

Sincerely,

/RA/ J. Downs for

Brian W. Smith, Chief
Uranium Enrichment Branch
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

The NRC staff also acknowledges the lack of understanding expressed by licensees concerning the cyber security threat. A cyber security "threat conference" is currently being planned to have both government and private sector experts better inform licensees of current cyber threats and risks. More information, discussion, and coordination of this conference can be expected within the next few months.

If you have any questions, I can be reached at 301-492-3137, or via e-mail at brian.smith@nrc.gov.

Sincerely,

/RA/ J. Downs for

Brian W. Smith, Chief
Uranium Enrichment Branch
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

DISTRIBUTION:

FCSS r/f	UEB r/f	JKinneman/NMSS	CLui/NSIR
MBailey/NMSS	PHabighorst/NMSS	MLayton/NSIR	CErlanger/NSIR
RRichardson/NSIR	ASapountzis/NSIR	LHarris/NSIR	RCostello/NSIR
DParsons/NSIR	GSimonds/NSIR	MShin/NSIR	

ML12328A108

OFFICE	NMSS/FCSS/UEB	NMSS/FCSS/UEB	NSIR/DSP/FCTSB	NMSS/FCSS/UEB
NAME	JDowns	TRichmond	RCaldwell *via e-mail	BSmith /J. Downs for/
DATE	11/27/12	11/27/12	11/ 27/12	11/27/12

OFFICAL RECORD COPY

Sexton, Kimberly

From: ZORN, Jason [jcz@nei.org]
Sent: Wednesday, June 27, 2012 8:48 AM
To: Sexton, Kimberly
Subject: RE: The Jack/Jason Post 9/11 Security Extravaganza
Attachments: OGC Security Seminar (Apr 2010).pdf; OGC Security Seminar (Zorn Speaker Notes) (Apr 2010).pdf

Per your request. This is everything I have.

From: Sexton, Kimberly [mailto:Kimberly.Sexton@nrc.gov]
Sent: Tuesday, June 26, 2012 4:49 PM
To: ZORN, Jason
Subject: The Jack/Jason Post 9/11 Security Extravaganza

Hi there,

For some reason I seem to have deleted my saved copies of the Jack/Jason Post 9/11 Security presentation that ya'll did for OGC two years ago. I can't find it in ADAMS either. Do you have an e-copy saved that you could easily send to me? If not I can ask Trip.

Thanks!

Kimberly A. Sexton
Legal Counsel
Office of Commissioner William C. Ostendorff
U.S. Nuclear Regulatory Commission
(301) 415-3599 (office)
(b)(6) (mobile)
(301) 415-1757 (fax)
Kimberly.Sexton@nrc.gov

Security Seminar Schedule

Part 1 (8:30 - 9:45 = 1 hour, 15 minutes)

Subject	Minutes	Time
Welcome/Format	5	8:30 – 8:35
I. Primitive Pre-9/11 Security	5	8:35 – 8:40
II. Fundamental Elements	10	8:40 – 8:50
III. BIG BANG Expansion	15	8:50 – 9:05
IV. Intelligent Design	5	9:05 – 9:10
V. Public Information & Secrecy	10	9:10 – 9:20
VI. Rulemaking vs. Orders	5	9:20 – 9:25
VII. Energy Policy Act	10	9:25 – 9:35
VIII. National Security	5	9:35 – 9:40
IX. & X. Current Threats & Dangers	5	9:40 – 9:45
Intermission	10	9:45 – 9:55

Part 2 (9:55 - 11:25 = 1 hour, 30 minutes)

1. Introduction 5 9:55 – 10:00
2. SGI/Fingerprinting 15 10:00 – 10:15
3. Cyber Security 15 10:15 – 10:30
4. Aircraft Threats 15 10:30 – 10:45
5. SNM Security 10 10:45 – 10:55
6. Licensing/Security Issues 5 10:55 – 11:00
7. Reactor Security 10 11:00 – 11:10
8. RTR Security 5 11:10 – 11:15
9. ISFSI Security 5 11:15 – 11:20
10. Security During Construction 5 11:20 – 11:25

U.S.NRC

Protecting People and the Environment

THE SECURITY OF NUCLEAR FACILITIES AND MATERIALS IN THE POST-9/11 ENVIRONMENT: THE EVOLUTION FROM PRIMITIVE TO INTELLIGENT DESIGN

April 7, 2010

Jack R. Goldberg, Special Counsel
Office of the General Counsel
United States Nuclear Regulatory Commission

Jason Zorn, Attorney
Office of the General Counsel
United States Nuclear Regulatory Commission

U.S.NRC

Agenda

I. The Primitive Pre-9/11 Security Requirements
II. Fundamental Elements of Pre-9/11 Security
III. The Big Bang Expansion of the Terrorists' Universe: Changes from 9/11
IV. Intelligent Design: Aircraft and Cyber
V. Protection of Information

U.S.NRC

Agenda (Con't)

VI. Rulemaking vs. Orders
VII. The Energy Policy Act of 2005
VIII. National Response Framework/National Infrastructure Protection Plan
IX. Current Threat Environment
X. Caution: Danger Ahead

U.S.NRC

The "Primitive" Pre-9/11 Security Requirements

- 3G's of Reactor Security–Guns, Guards & Gates
- Materials "Insecurity"
- Cyberless Security
- Missiles from Cuba–Enemies of the United States
- NRC's Invention of the Design Basis Threat (DBT)
- Legal Restrictions on Agreement States' Security Role
- The NRC: Who's on First? What's on Second?

U.S.NRC

Fundamental Elements of Pre-9/11 Security

- The Design Basis Threat
  - Radiological Sabotage of Power Reactors
  - Theft or diversion of SNM (Cat I Facilities)
  - Adversary Characteristics
- Enemies of the United States (50.13)
- Physical Security
- Access Authorization
- Inspection and Enforcement/Force on Force
- "High Assurance" Performance Standard

U.S.NRC

Pre-9/11 Security (Con't)

- Safeguards Information and its Limitations
- Research and Test Reactors
- Materials Security
  - Cat I Facilities
  - ISFSIs
  - Transportation
  - Other Materials

U.S.NRC

The BIG BANG Expansion of the Terrorists' Universe: The September 11, 2001 Attack on the United States

Formation of Response to Terrorist Attack (RTA) Task Force

Comprehensive Review

U.S.NRC

Results of the September 11, 2001 Attack

- Organizational Developments
  - DHS and National Response Framework
  - NRC: NSIR and OGC
  - OGC's Role: Legal and Policy Issues

U.S.NRC

Results of the September 11, 2001 Attack

- Reactor Security Orders
  - Interim Compensatory Measures (ICM)
  - Design Basis Threat (DBT)
  - Access Authorization
  - Guard Training and Qualification
  - Fatigue

U.S.NRC

Results of the September 11, 2001 Attack

- State of the Art Power Reactor Security
  - Physical Security
  - Access Authorization
  - Training and Qualification
  - Safeguards Contingency Plans
  - Cyber Security Plans
  - Deadly Force
  - Remotely Operated Weapons Systems
  - Insider Mitigation
  - Force-on-Force Testing
  - Safety/Security Interface

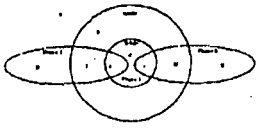
U.S.NRC

Results of the September 11, 2001 Attack

- Aircraft Attacks on Nuclear Power Facilities
  - Imminent Threat Procedures
  - Mitigative Measures for Large Fires and Explosions
  - Aircraft Impact Assessment Rule

U.S.NRC

Results of the September 11, 2001 Attack



U.S.NRC

Results of the September 11, 2001 Attack

- Research and Test Reactors
  - AEA 104c Requires Minimum Regulation to Assure Safety
  - Sabotage DBT Applies to RTRs greater than or = 2MW
  - CALs to most RTRs
  - Security Assessments: No Credible Sabotage or Theft Results in Significant Radiological Consequences
  - Compensatory Measures Incorporated into RTR Security Plans or Procedures
  - Fingerprinting Orders for Unescorted Access or Access to SGI

U.S.NRC

Results of the September 11, 2001 Attack

- Materials Security
  - Cat I Facilities
  - Enrichment Facilities
  - ISFSIs
  - Mixed Oxide Fuel Facilities
  - Other Licensees/Facilities
  - Material Control and Accountability
  - Transportation of Spent Fuel and RAMQC
  - Agreement State Licensees

U.S.NRC

Results of the September 11, 2001 Attack

- Safeguards Information Expansion
- Fingerprinting and FBI Criminal History Records Checks
- Licensing New Facilities: The Adequate Protection Dilemma

U.S.NRC

Intelligent Design

- Relationship Between Facility Design and Security Requirements
- The Aircraft Impact Assessment Rule
- Cyber Security

U.S.NRC

The Tension Between Public Information/ Involvement and Government/NRC "Secrecy"

- Classified Information
- Safeguards Information
- SUNSI/CUI/SBU/UCNI
- "No comment" Policy
- First Amendment Issues
- Investigatory and Enforcement Issues

U.S.NRC

Rulemaking vs. Orders

- Commission Policy Position
- DBT Order Litigation
- Current Status of Orders
- Current Status of Rulemaking

U.S.NRC

Energy Policy Act of 2005

- DBT Rulemaking
- Expansion of Fingerprinting Authority
- Enhanced Weapons
- Introduction of Dangerous Weapons
- Force-on-Force Exercises
- Sabotage of Nuclear Facilities
- DHS Consultations for Siting of New Reactors
- Byproduct Material Security
  - Import/export controls
  - National Source Tracking System
  - Task Force on Radiation Source Protection and Security

U.S.NRC

NRC Involvement in National Security

- Intelligence Sharing
- National Response Framework
  - National Infrastructure Protection Plan (NIPP)
  - Support Annexes

U.S.NRC

Closing Issues

- The Current Threat Environment
- CAUTION: DANGER AHEAD
- "Senators Warned of Terror Attack on U.S. by July," NY Times, Feb. 3, 2010
- "To win the cyber-war, look to the Cold War," Washington Post, Feb. 28, 2010

U.S.NRC

Thank you

End of Part I

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

CURRENT AND FUTURE ISSUES IN SECURITY

April 7, 2010

Jack R. Goldberg, Special Counsel
Office of the General Counsel
United States Nuclear Regulatory Commission

Jason Zorn, Attorney
Office of the General Counsel
United States Nuclear Regulatory Commission

OFFICIAL USE ONLY – ATTORNEY WORK PRODUCT

U.S.NRC

Agenda

- Introduction/Overview
- Safeguards Information & Fingerprinting
- Cyber Security
- NRC's Treatment of Aircraft Threats
- Special Nuclear Materials Security

U.S.NRC

Agenda (Con't)

- Licensing and Imposition of Updated Security Requirements
- Reactor Security: Force-on-Force, Enhanced Weapons, Remote Operated Weapons Systems (ROWS)
- Research and Test Reactor Security
- Security of ISFSIs
- Security During Construction

U.S.NRC

Introduction

- Introduction/Overview
- Current and Future Threat Environment
- NRC's Potential Reversion to Pre-9/11 Mode

U.S.NRC

Safeguards Information and Fingerprinting

- AEA Sections 147 & 149
- Pre-(EPAct of 2005) Regulations
- Post-9/11 Deficiencies in NRC Regulations
- EPAct of 2005 Amendments
- EPAct Implementation via Orders
- SGI & SGI-M
- Access to the Aircraft Impact Data

U.S.NRC

Safeguards Information and Fingerprinting (Con't)

- Reviewing Officials (ROs); Trustworthiness and Reliability (T&R) Officials
- Agreement State Issues
- Relief from Fingerprinting
  - Access to SGI (73.59)
  - Access to Materials/Property (73.61)

U.S.NRC

Safeguards Information and Fingerprinting (Con't)

- SGI/Fingerprinting Issues in Need of Commission Resolution and Rulemaking:
  - RO/T&R Official
  - Need to Know Definition
  - Access to SGI in Non-NRC Proceedings/Contexts
  - Foreign National Access to SGI
  - Federal Security Clearance Acceptance
  - Periodic Reinvestigations
  - Removal of SGI from the United States
  - Scope of NRC Adjudications of Access to SGI
  - NRC Staff Reviews/Approvals of SGI Programs
  - Fingerprinting Relief Rules Changes
  - Pending Legislative Request

U.S.NRC

Cyber Security

- Development of Cyber Security Rule
- Scope of the Rule
- Cyber Security Plans
- Interaction with FERC/NERC

U.S.NRC

NRC's Treatment of Aircraft Threats

- ICM Order B.5.b.
- Mitigating Strategies Rule (50.54(hh))
- DBT Rule
- Aircraft Impact Assessment Rule (50.150)

U.S.NRC

Special Nuclear Materials Security

- Material Categorization
- Category I Facility Denial Strategy Order
- New Enrichment Facilities – CI Programs
- MOX Facility

U.S.NRC

Special Nuclear Materials Security (Con't)

- Material Categorization
  - Current Scheme: KISS (Keep It Simple Stupid)--Only 3 Categories of SNM
  - Type and Quantity of Material Insufficient for Risk-Informed, Graded Security Regulations
  - Staff's Proposed Approach: Attractiveness of Material Based on IND Threat
  - Factors: Form (oxide, solution, solid); Weight % of SNM; Radiation Level
  - Levels: A = Pure Products; B = High-Grade; C = Low-Grade; D = All Other Materials

U.S.NRC

Special Nuclear Materials Security (Con't)

- Category I Facility Denial Strategy Order
  - Cat. I Facility SNM Issue
  - Theft and/or Diversion DBT
  - Order Imposing Performance-Based Denial Strategy
  - SECRET-RD Basis
  - Impact on Cat. I facilities

U.S.NRC

Special Nuclear Materials Security (Con't)

- New Enrichment Facilities – Counter-Intelligence Programs
  - Laser Enrichment Superior to Gas Centrifuge Process
  - Laser Enrichment Technology is Highly Classified & Subject to International Agreements
  - Proliferation Concerns
  - Limited NRC Employee Access to Most Sensitive Information
  - US Government (DOE, FBI) Supports Counterintelligence (CI) Program for Laser Technology
  - NRC Staff Proposes CI Program for Enrichment Technology (SECY-09-0166, Nov. 5, 2009)

U.S.NRC

Special Nuclear Materials Security (Con't)

- MOX Facility
  - MOX Fuel Fabrication Facility on DOE Property but operated by DOE Contractor
  - Strom Thurmond National Defense Authorization Act for Fiscal Year 1999-ERA Amendment
  - NRC License/Regulation Required
  - Draft MOU w/NNSA-DOE
  - Who Should Be the Licensee?
  - Who Should be the Cognizant Security Agency (CSA)?
  - Whose DBT and Other Security Requirements Should Apply?
  - DOE's HRP/Polygraph Requirement and Two-Person Rule
  - Who Should Provide the Guard Force?
  - Inspection and Enforcement Issues
  - Price-Anderson, Decommissioning, Transportation Issues
  - Note from Kimberly Sexton to Steve Burns, March 5, 2010 (West ltm)

U.S.NRC

Licensing and Imposition of Updated Security Requirements

- The Adequate Protection Dilemma
- Licensing Requirements; Hearing Issues--AEA 182; See, e.g., 10 C.F.R. 50.35. 50.40, 50.50, 70.31(a), (d)
- Imposition of Adequate Protection Security Requirements
- The "LES" SRM (SECY-03-083, July 2, 2003)
- The "Perfect Solution"

U.S.NRC

Reactor Security

- Force-on-Force Exercises
- Enhanced Weapons/Firearms Background Checks
- Remotely Operated Weapon Systems (ROWS)
- Changes to Security Plans

U.S.NRC

Research and Test Reactor Security

- Overview of Commission Policy/Regulatory Strategy
- Post-9/11 Actions
- GAO Report

U.S.NRC

Security of ISFSIs

- Post 9/11 Orders
- Problems with Regulations
- Rulemaking Plan/Change in Protection Strategy

U.S.NRC

Security During Reactor Construction

- Rejection of Pre-Operational Security Design Assessments
- Initiation of Rulemaking
- Fingerprinting Issues

U.S.NRC

Thank you!

~~OFFICIAL USE ONLY—ATTORNEY WORK PRODUCT~~

The Security of Nuclear Facilities and Materials in the Post-9/11 Environment

The Evolution from Primitive to Intelligent Design

&

Current & Future Issues

OGC Seminar 2010

Jack R. Goldberg

Jason Zorn

~~OFFICIAL USE ONLY-- ATTORNEY WORK PRODUCT~~

The Security of Nuclear Facilities and Materials in the Post-9/11 Environment
The Evolution from Primitive to Intelligent Design

Jack R. Goldberg
OGC Seminar 2010

I. The "Primitive" Pre-9/11 Security Requirements

II. Fundamental Elements of Pre-9/11 Security–10 C.F.R. Part 73

A. The Design Basis Threat (DBT)

1. Radiological Sabotage of Power Reactors (73.1(a)(1))

2. Theft and Diversion of Special Nuclear Material (SNM); Category I Facilities (73.1(a)(2))

3. Adversary Characteristics (The "ACD")

B. Enemies of the United States (10 C.F.R. § 50.13)

C. Physical Security (73.55)

D. Access Authorization (73.56) & Fingerprinting (73.57, 73.61)

E. Inspection & Enforcement; Force-On-Force (FOF) Exercises

F. The "High Assurance" Performance Standard (73.55)(b))

G. Safeguards Information and Its Limitations (AEA § 147; Part 73)

H. Research & Test Reactors (RTRs) (AEA § 104c)

I. Materials Security

1. Category I Facilities (73.2 definition of a "Formula Quantity")

2. Independent Spent Fuel Storage Facilities (ISFSIs)

3. Transportation of Spent Fuel and Other Radioactive Materials

4. Other Materials Security

III. The BIG Bang's Expansion of the Terrorists' Universe: The September 11, 2001 Attack on the United States

A. Organizational Developments

1. DHS and the National Response Framework
2. NRC: NSIR & OGC
3. OGC's Role: Legal and Policy Issues

B. Substantive Security Developments

1. Order Imposing Interim Compensatory Measures (ICM Order, Feb. 25, 2002)
2. The DBT Order (April 29, 2003)
3. The Guard Training & Qualification Order; The Fatigue Order (April 29, 2003)
4. State of the Art Power Reactor Security
    a. Physical Security (73.55(c)(3))
    b. Access Authorization (73.56)
    c. Guard Training & Qualification (73.55(c)(4))
    d. Safeguards Contingency Plans (73.55(c)(5))
    e. Cyber Security Plans (73.55(c)(6))
    f. Deadly Force (73.55(k)(3))
    g. Remotely Operated Weapons Systems (ROWS)
    h. Insider Mitigation (73.55(b)(9))
    i. Force-on-Force Testing
    j. Safety/Security Interface (73.58)
5. Aircraft Attacks on Nuclear Power Facilities
    a. Imminent Threat Procedures (ICM B.5.a.; 50.54(hh)(1))
    b. Mitigative Measures for Large Fires & Explosions (ICM B.5.b.; 50.54(hh)(2))

c. The Aircraft Impact Assessment Rule (50.150)

6. Research & Test Reactors (AEA § 104c)

a. AEA 104c Requires Minimum Regulation to Assure Safety

b. Sabotage DBT Applies to RTRs greater than or = 2MW

c. CALs to most RTRs

d. Security Assessments: No Credible Sabotage or Theft Results in Significant Radiological Consequences

e. Compensatory Measures Incorporated into RTR Security Plans or Procedures

f. Fingerprinting Orders for Unescorted Access or Access to SGI

7. Materials Security

a. Category I Facilities

b. Enrichment Facilities

c. Independent Spent Fuel Storage Facilities (ISFSIs)

d. Mixed Oxide Fuel Facilities (MOX)

e. Other Materials Licensees (GDPs, Fuel Fabrication Facilities, M&Ds, Large Irradiators, etc.)

f. Material Control and Accounting (MC&A)

g. Transportation of Spent Fuel & RAMQC

h. The Agreement State Program–Safety vs. Security (AEA § 274)

i. The "Increased Control" (IC) Licensees

C. Safeguards Information Expansion (AEA § 147; 73.21, 73.22, 73.23)

1. Safeguards Information (SGI) (73.22)

2. Safeguards Information–Modified Handling (SGI-M) (73.23)

3. Access to the Aircraft Impact Data

D. Fingerprinting and FBI Criminal History Records Checks (CHRC) (AEA § 149)

1. Unescorted Access to Facilities and Materials

2. Access to SGI

3. Relief from Fingerprinting (73.59, 73.61); Security Clearance Recognition

4. The Reviewing Official (RO) & the Trustworthy & Reliability (T&R) Official

E. Licensing New Facilities–The Adequate Protection Dilemma (SECY-03-0083 SRM (July 2, 2003))

IV. Intelligent Design

A. The Relationship between Facility Design and Security Requirements

B. The Aircraft Impact Assessment Rule (50.150)

C. Cyber Security

1. The DBT

2. The Cyber Security Rule (73.54)

3. FERC's Authority and CIP Standards; The MOU w/NERC

4. The NRC's Cyber Security Authority

a. OGC Memo to Commission (Mar. 8, 2010)

b. Note to File from Goldberg & Zorn (Mar. 9, 2010)

V. The Tension between Public Information/Involvement and Government/NRC "Secrecy"

A. Classified Information (Executive Orders 12958, 12968, 13526)

1. Top Secret, Secret, Confidential

2. Restricted Data (AEA §§ 11y, 141, 142)

3. Special Access Programs (SAPs)

B. Safeguards Information (SGI) (AEA § 147)

1. AEA and NRC Regulations: Scope & Limitations (AEA § 147; Part 73)

2. Fingerprinting and FBI Criminal History Records Checks (CHRCs) (73.57)

3. Relief from Fingerprinting & CHRCs (73.59); Security Clearances

4. Aircraft Impact Data; Foreign National Access to SGI (Order to New Reactor Vendors: EA-07-231 (Sept. 12, 2007), 72 Fed. Reg. 53,797 (Sept. 20, 2007))

5. Unauthorized Disclosures of SGI; Civil & Criminal Sanctions (SGI RIS 2003-08 (April 30, 2003))

6. Access to SGI & SUNSI in NRC Proceedings (2.307(c), 2.311(a)(3))

7. Access to SGI in Non-NRC Proceedings

C. SUNSI; CUI; SBU; UCNI

D. The US Government and NRC "No Comment" Policy (DG-SGI-1)

E. First Amendment Issues

F. Investigatory and Enforcement Issues

VI. Rulemaking vs. Orders

A. DBT Order Litigation

B. Current Status of Orders

1. Reactors

2. Materials

3. SGI & Fingerprinting

C. Current Status of Rulemakings

VII. The Energy Policy Act of 2005

A. DBT Rulemaking

B. Fingerprinting (AEA § 149; 73.57, 73.59, 73.61)

C. Enhanced Weapons (74 Fed. Reg. 46,800 (Sept. 11, 2009)

D. Introduction of Dangerous Weapons into NRC-Regulated Facilities (73.75, 73.81)

OFFICIAL USE ONLY-- ATTORNEY WORK PRODUCT

The Security of Nuclear Facilities and Materials: Current & Future Issues

Jack R. Goldberg & Jason Zorn
OGC Seminar 2010

1. Introduction and Overview

   The Current and Future Threat Environment—CAUTION: DANGER AHEAD

   NSIR and NRC's Potential Reversion to Pre-9/11 Mode

2. Safeguards Information & Fingerprinting

   Atomic Energy Act Sections 147 (Safeguards Information (SGI)) & 149 (Fingerprinting)

   NRC's Pre-(EPAct of 2005) Regulations—Power Reactor Requirements Only

   Post-9/11 Deficiencies in NRC Regulations

   EPAct of 2005 Amendments to the AEA

   EPAct Implementation via Orders

   The New, Expanded SGI Regulations (73.21, 73.22, 73.23)

   Access to the Aircraft Impact Data

   Currently-Valid Orders Imposing Requirements Not Addressed by NRC Regulations

   NRC's Recent Legislative Proposals

   Continued Need to Regulate SGI by Order

   Legal Issues Associated with Safeguards Information & Fingerprinting

   SGI/Fingerprinting Issues in Need of Commission Resolution & Rulemaking

3. Cyber Security

   The DBT

   The Cyber Security Rule (10 C.F.R. 73.54); Cyber Security Plans

   FERC's Authority and CIP Standards; The MOU w/NERC

   The NRC's Cyber Security Authority

4. NRC's Treatment of Aircraft Threats

   ICM Order B.5.b.; Mitigating Strategies Rule (10 C.F.R. 50.54(hh))

   DBT Rule (10 C.F.R. 73.1)

   Aircraft Impact Assessment Rule (10 C.F.R. 50.150)

5. Special Nuclear Materials Security

   Material Categorization

   Cat. I Facility Denial Strategy Order

   New Enrichment Facilities—Counter-Intelligence Programs for Enrichment Technology

   MOX Facility

6. Licensing and Imposition of Updated Security Requirements

   The Adequate Protection Dilemma

   The "Perfect" Solution

7. Reactor Security

   FOF

   Enhanced Weapons

   Remotely Operated Weapons Systems (ROWS)

8. Research & Test Reactors

9. Security of ISFSI's

10. Security During Construction (Access Authorization and Fitness for Duty)

~~OFFICIAL USE ONLY-- ATTORNEY WORK PRODUCT~~

SAFEGUARDS INFORMATION AND FINGERPRINTING ISSUES

Jack R. Goldberg
OGC Seminar 2010

The Evolution of Atomic Energy Act and NRC Requirements

Atomic Energy Act Sections 147 (Safeguards Information (SGI)) & 149 (Fingerprinting)

NRC's Pre-(EPAct of 2005) Regulations—Power Reactor Requirements Only

Post-9/11 Deficiencies in NRC Regulations

- Scope Limited to Power Reactor Licensees
- Defined to Exclude Byproduct Materials and Materials Licensees
- Access Limited to Prescribed Categories of Persons or as Approved by Commission
- No Trustworthy & Reliability Requirement for Persons Granted Access
- Regulations Assumed Bona Fide Licensee Access Decisions
- SGI Protection Requirements Not Suited to Materials Licensees
- Fingerprinting Authority Limited to Access to SGI via Power Reactor Licensees
- Did Not Address Foreign Nationals' (and Similar Others') Access to SGI
- Did Not Address Access to SGI in NRC or Non-NRC Proceedings
- RO & T&R Official Fingerprinting Restrictions
- Loss of NRC Control of SGI in Hands of Others

EPAct of 2005 Amendments to the AEA

- Expanded Fingerprinting Authority
- Mandated Fingerprinting on Immediately Effective Basis
- Relief from Fingerprinting (& FBI Criminal History Records Check) by Rule Only

EPAct Implementation via Orders

- Orders Based on NRC's Common Defense and Security Authority

Issued to Materials Licensees in Risk-Informed Order

Issued to NRC Licensees by NRC

Issued by NRC to Agreement State Licensees—Dual Regulation

Reviewing Officials (ROs) Adjudicated by NRC

Safeguards Information—Modified Handling (SGI-M) Requirements

Access to the Aircraft Impact Data: The Order to New Reactor Vendors (EA-07-231 (Sept. 12, 2007), 72 Fed. Reg. 53,797 (Sept. 20, 2007))

Agreement States' Opposition:

Common Defense and Security Basis

Dual Regulation

Increased Control Orders based on Public Health and Safety

Issued by NRC to NRC Licensees

Compatible Requirements Issued by Agreement States to Their Licensees

Trustworthy and Reliability (T&R) Officials

No Fingerprinting of T&R Officials

Current NRC SGI & Fingerprinting Requirements

The New, Expanded SGI Regulations (73.21, 73.22, 73.23)

Safeguards Information (SGI) (73.22)

Safeguards Information–Modified Handling (SGI-M) (73.23)

Trustworthiness & Reliability based on Background Checks Required for Access to SGI

Fingerprinting & FBI Criminal History Records Checks

Employment History

Education

Personal References

Fingerprinting and FBI Criminal History Records Checks (73.57)

Relief from Fingerprinting & FBI Criminal History Records Checks

Access to SGI (73.59)

Access to Materials/Property (73.61)

Federal Security Clearance Recognition for Unescorted Access to Power Reactors (73.57)(b)(2)(i)) but Not for Access to SGI (73.57)9b)(2)(ii)

Access to SGI (& SUNSI) in NRC Proceedings (2.307(c), 2.311(a)(3))

Access to the Aircraft Impact Data

Currently-Valid Orders Imposing Requirements Not Addressed by NRC Regulations

NRC's Recent Legislative Proposals

Authorization to Fingerprint T&R Officials Who Do Not Require Access to SGI or Materials

Continued Need to Regulate SGI by Order

RO's & T&R Officials

Foreign National Access to Aircraft Data SGI

Legal Issues Associated with Safeguards Information & Fingerprinting

AEA and NRC Regulations: Definition & Scope Limitations (AEA § 147; Part 73)

Unauthorized Disclosures of SGI; Civil & Criminal Sanctions (SGI RIS 2003-08 (April 30, 2003))

The US Government and NRC "No Comment" Policy (DG-SGI-1)

First Amendment Issues

Investigatory and Enforcement Issues

Access to SGI in Non-NRC Proceedings

The Government's New CUI Policy

SGI/Fingerprinting Issues in Need of Commission Resolution & Rulemaking

RO/T&R Official

Need to Know Definition

Access to SGI in Non-NRC Proceedings/Contexts

Foreign National Access to SGI

Federal Security Clearance Acceptance

Periodic Reinvestigations

Removal of SGI from the United States

Scope of NRC Adjudications of Access to SGI

NRC Staff Reviews/Approvals of SGI Programs

Fingerprinting Relief Rules Changes

- New or Different Categories Needed
- Conditions of Categories Need to be Made Consistent
- Consistency Needed between Relief for Access to SGI and Unescorted Access

Loss of NRC Control of SGI in Hands of Others

Pending Legislative Request

Slide 6: Cyber Security
Jason Zorn

- Development of Cyber Security Rule
  - 2002 ICM Order:
    - reference to cyber
    - licensees only required to assess vulnerabilities
  - 2003 DBT Order
    - reference to cyber in context of insider threat
  - NEI 04-04
    - *Voluntary industry initiative for uniform cyber protection standards*
    - Limited in scope; Assessment but no protection
    - Not tied to any regulatory requirement; unenforceable
  - 2006 Proposed Power Rector Security Rulemaking
    - Proposed 73.55(m): protection of digital equipment and systems
  - 2007 Final DBT Rule
    - Included "cyber attack" as element of the DBT
    - Not included in the 2005 proposed rule
    - Required to be "considered' in EPAct 2005
  - 2009 Final Power Reactor Security Rule
    - "Cyber Security Rule": 73.54
    - Separate section of the regulation to accommodate other classes of licensees (currently only applied to power reactors)
    - Broad, programmatic requirements
  - Regulatory Guide 5.71
  - Industry Guidance (NEI 08-09)

- Scope of the Rule
  - Scope of rule limited by application of Part 73 security requirements
  - digital systems or networks with safety-related, important-to-safety, security, or emergency preparedness functions
  - Part 73 focused on "radiological sabotage" for reactors (significant core damage)
  - Rule only applies to equipment that, if comprised could directly or indirectly result in radiological sabotage
  - Does not include equipment without potential for radiological sabotage, even if the equipment is subject to safety regulations

- Cyber Security Plans
  - Required to be submitted by operating reactors NLT November 23, 2009
  - New reactors required to amend application after effective date
  - Cyber Security plan one of 4 plans required by 50.54; part of license
  - NRC and industry separately developed generic templates
    - Mix of who is using what template so far
    - Staff is currently performing acceptance review for cyber security plan submittals
  - Submittals used a variety of templates

- Some based on NEI versions that the staff had not endorsed; resulted in significant numbers of RAIs
- Staff working with industry to resolve RAIs either generically or on a site by site basis
- Implementation schedule
  - No time specified in the rule
  - Staff late in developing guidance on what an acceptable schedule is

- Interaction with FERC/NERC
  - Relationship between FERC and NERC/what is NERC?
  - FERC Critical Infrastructure Protection Order
    - Nuclear exemption
    - Revision; NRC and industry comments
    - Publication of revision
      - Exemption process for equipment under NRC cyber requirements
  - Memorandum of Understanding
    - MOU with NERC (as opposed to FERC)
    - Attempts to mitigate dual regulation, conflict, etc.
    - Describes authorities of NRC and NERC
    - Describes exemption process and coordination role
    - Unable to include reimbursement clause for NRC to conduct inspections on behalf of NERC (Economy Act restrictions)

~~OFFICIAL USE ONLY – ATTORNEY WORK PRODUCT~~

NRC's TREATMENT OF AIRCRAFT THREATS

Jack R. Goldberg
OGC Seminar 2010

ICM Order B.5.b.

Venn Diagram (Attached)

Mitigating Strategies Rule (10 C.F.R. 50.54(hh)(2))

Requires strategies to maintain and restore

core cooling

containment

spent fuel pool cooling capabilities

under conditions associated with loss of large areas of the plant due to explosions or fire, to include strategies in the following areas:

fire fighting

operations to mitigate fuel damage

actions to minimize radiological release

DBT Rule (10 C.F.R. 73.1(a))

"(1) Radiological Sabotage . . . [includes] . . . (v) A cyber attack."

"(2) Theft or diversion of formula quantities of strategic special nuclear material . . . [includes] . . . (v) A cyber attack."

Aircraft Impact Assessment Rule (10 C.F.R. 50.150)

Applies to New CPs, OLs, Design Certifications, COLs (See rule)

Assessment Required of Effects of Impact of Large Commercial Aircraft

Realistic Analysis Must Be Used

Identification & Incorporation of Design Features, with Reduced Operator Actions, to Show:

- Reactor Core Remains Cooled, or Containment Remains Intact, and
- Spent Fuel Cooling or Spent Fuel Pool Integrity is Maintained

Aircraft Impact Characteristics

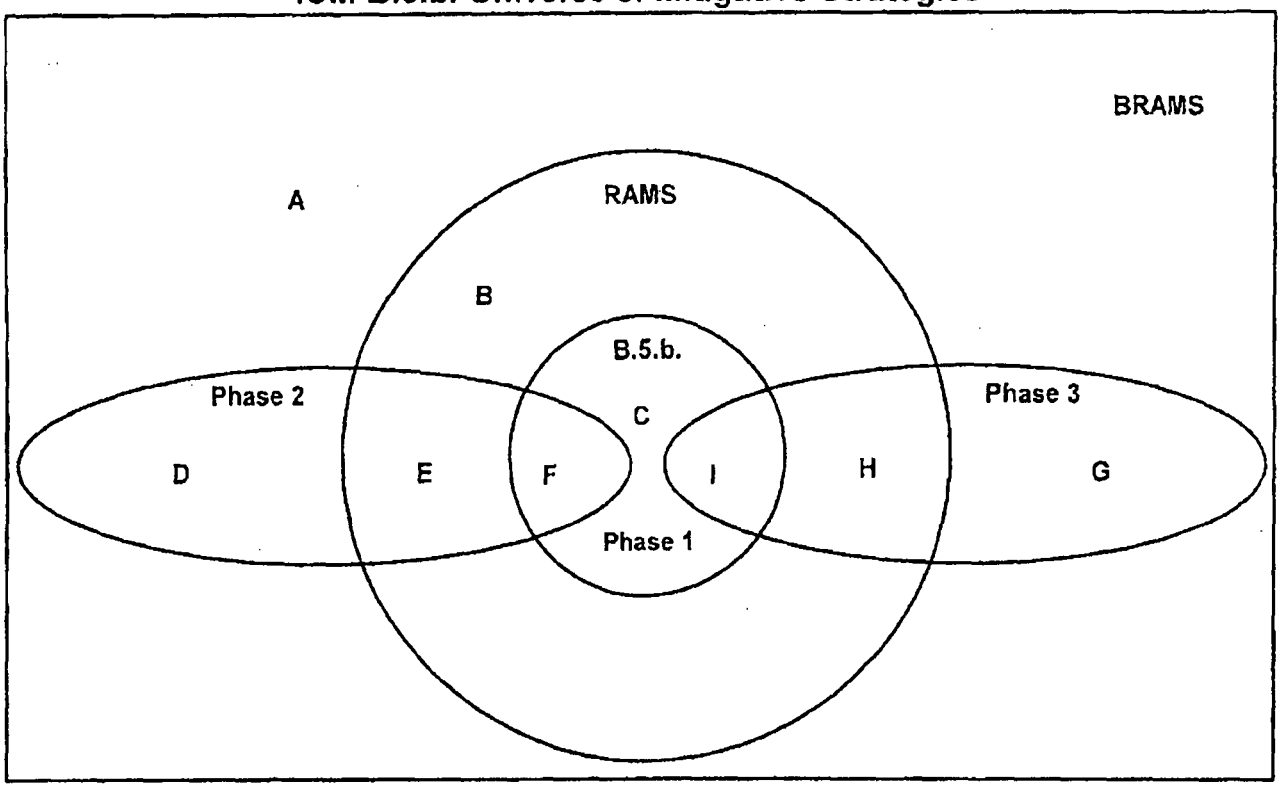
- Beyond Design-Basis Impact
- Large, Commercial Aircraft, Long-Distance Flights in US with Full Fuel Loading
- Impact Speed & Angle of Impact from Experienced & Inexperienced Pilots
- Control at Low Altitude Representative of Nuclear Plant's Low Profile

Content of Application

- Design Features and Functional Capabilities Identified by Assessment
- How Above Features & Capabilities Meet Assessment Requirements

Control of Changes

ICM B.5.b. Universe of Mitigative Strategies



Key to Elements of Sets Related to ICM B.5.b.

A = A mitigative strategy not employing existing or readily available resources ("BRAMS")

B = A mitigative strategy employing existing or readily available resources ("RAMS")

C = A RAMS within the scope of B.5.b. ("B.5.b. RAMS") identified in Phase 1

D = A mitigative strategy indentified in Phase 2 not employing existing or readily available resources ("Phase 2 BRAMS")

E = A mitigative strategy identified in Phase 2 employing existing or readily available resources but outside the scope of B.5.b. ("Phase 2 RAMS")

F = A mitigative strategy identified in Phase 2 employing existing or readily available resources and within the scope of B.5.b. ("Phase 2 B.5.b. RAMS")

G = A mitigative strategy identified in Phase 3 not empoying existing or readily available resources ("Phase 3 BRAMS")

H = A mitigative strategy identified in Phase 3 employing existing or readily available resources but outside the scope of B.5.b. ("Phase 3 RAMS")

I = A mitigative srategy identified in Phase 3 employing existing or readily available resources and within the scope of B.5.b. ("Phase 3 B.5.b. RAMS")

Note: Mitigative Strategies C, F and I are enforceable since they are within the scope of B.5.b. and its implementing guidance dated February 25, 2005. Mitigative strategies B, E, and H are outside the scope of B.5.b., and thus are not required, but could be required by the Commission through issuance of an order or rulemaking. Since B, E, and H are RAMS, they either can be determined to be necessary for adequate protection or, if not, would satisfy the backfit rule. Mitigative Strategies A, D and G are BRAMS but could be required if deemed to be necessary for adequate protection or, if not a matter of adequate protection, if they satisfy the backfit rule; if neither however, they may be referred to DHS.

~~OFFICIAL USE ONLY-- ATTORNEY WORK PRODUCT~~

SPECIAL NUCLEAR MATERIALS SECURITY

Jack R. Goldberg
OGC Seminar 2010

Material Categorization

Current Scheme: KISS (Keep It Simple Stupid)--Only 3 Categories of SNM

Type and Quantity of Material Insufficient for Risk-Informed, Graded Security Regulations

Staff's Proposed Approach: Attractiveness of Material based on IND Threat

Factors: Form (oxide, solution, solid); Weight % of SNM; Radiation Level

Levels: A = Pure Products; B = High-Grade; C = Low-Grade; D = All Other Materials

Cat. I Facility Denial Strategy Order

Cat. I Facility SNM Issue

Theft and/or Diversion DBT

Order Imposing Performance-Based Denial Strategy

SECRET-RD Basis

Impact on Cat. I facilities

New Enrichment Facilities—Counter-Intelligence Programs for Enrichment Technology

Laser Enrichment Superior to Gas Centrifuge Process

Laser Enrichment Technology is Highly Classified & Subject to International Agreements

Proliferation Concerns

Limited NRC Employee Access to Most Sensitive Information

US Government (DOE, FBI) Supports Counterintelligence (CI) Program for Laser Technology

NRC Staff Proposes CI Program for Enrichment Technology (SECY-09-0166, Nov. 5, 2009

MOX Facility

DOE-Contractor MOX Fuel Fabrication Facility on DOE Property

Strom Thurmond National Defense Authorization Act for Fiscal Year 1999--ERA Amendment

NRC License/Regulation Required

Draft MOU w/NNSA-DOE

Who Should Be the Licensee?

Who Should be the Cognizant Security Agency (CSA)?

Whose DBT and Other Security Requirements Should Apply?

DOE's HRP/Polygraph Requirement and Two-Person Rule

Who Should Provide the Guard Force?

Inspection and Enforcement Issues

Price-Anderson, Decommissioning, Transportation Issues

OFFICIAL USE ONLY-- ATTORNEY WORK PRODUCT

LICENSING AND IMPOSITION OF UPDATED SECURITY REQUIREMENTS

Jack R. Goldberg
OGC Seminar 2010

The Adequate Protection Dilemma

Licensing Requirements; Hearing Issues

AEA 182; *See, e.g.*, 10 C.F.R. 50.35. 50.40, 50.50, 70.31(a), (d)

Imposition of Adequate Protection Security Requirements

The "LES" SRM (SECY-03-083, July 2, 2003)

The "Perfect Solution"

~~OFFICIAL USE ONLY – ATTORNEY/CLIENT PRIVILEGE~~

Slide 16: Force-on-Force Exercises

Jason Zorn

- EPAct 2005 (Section 651) mandated that NRC conduct "security evaluations" at least every 3 years at Commission-designated facilities.
- Security evaluations "shall include" force-on-force" exercises
- Shall "to maximum extent practicable, simulate security threats in accordance with any design basis threat applicable to a facility."
- Requires annual report to Congress in classified and unclassified form

- Prior to 9/11, NRC had conducted force on force exercises at NPPs
- FOF includes "composite adversary team"
  - Team has capabilities consistent with the DBT
  - FOF evaluation includes 2 week assessment; 1st week walk through, tabletops, target set evaluation, etc.; 2nd week 3 FOF exercise
- CAF strategy to destroy complete target set
  - Target set is set of equipment or operator actions that, if prevented from performing safety function, would likely result in radiological sabotage
  - Target sets unique to each site

- FOF Enhancement Program
  - staff proposing changes to make the FOF program
  - Changes would take a more "holistic" approach to evaluating security
  - Go from "pass/fail" solely based on exercise results to weighing of other factors
  - Other factors include:
    - Officer training
    - Target set ID
    - Controller training and performance
  - Staff undergoing extensive evaluation, including public meetings and Congressional briefings
  - Criticisms:
    - From industry: changing the goalposts midgame (changes would make it easier to identify failures)
    - From public interest stakeholders: changes would make it easier to "cover up" failures because failure of exercise could potentially not result in overall failure
- New Reactor Force on Force
  - No requirement to complete FOF prior to operation
  - Staff is considering whether or not this is needed and how it would be imposed
  - If not prior to operation, then when? How long after is appropriate?

~~OFFICIAL USE ONLY – ATTORNEY/CLIENT PRIVILEGE~~

Slide 16: Enhanced Weapons/Firearms Background Checks

Jason Zorn

- EPAct 2005 section 653 (added section 161A)
- 4 Basic Provisions:
  - State law preemption
  - Authority for select licensees to use weapons and equipment illegal under Federal and state law (e.g. fully automatic weapons)
  - Conduct of NICS checks (Brady Bill) on all armed security officers
  - Development and issuance of "guidelines" approved by the AG
- Preemption and enhanced weapons both "voluntary"
- NICS checks mandatory
- Negotiation of guidelines with DOJ took nearly 4 years to complete. Guidelines issued in September 2009.
- Rulemaking
  - Proposed rule in October 2006 (prior to guidelines)
  - Proposed rule split from power reactor security rule in December 2008
  - Revised proposed rule to be issued soon
  - Final rule sometime early next year?

Slide 16: Remotely Operated Weapons Systems (ROWS)
Jason Zorn

- Increasing licensee interest in use of ROWS
  - Seen as a "force multiplier"
  - Reduces number of security officers
  - Reduces exposure of security officers
  - Potentially more accurate because of tracking, infrared, thermal
- Only one licensee currently using a system
- Legal and policy issues
  - Deadly force (defense of self/defense of others)
  - Safety (accurate target identification, control of malfunctions)
  - Reliable operability (harsh weather, mechanical malfunction)
  - Incorporation of "enhanced weapons"?

Slide 16: Changes to Security Plans
Jason Zorn

- Security plans (physical security, T&Q, Security contingency, cyber) part of the license per 50.54(p)
- Changes to security plans are changes to the license, thus requiring license amendment
- Except:
  - When changes do not decrease the effectiveness of the plan licensees may make changes without prior NRC approval
  - Requires notice to NRC and written description within 60 days of changes
- Common issues with plan changes:
  - Staff over-scrutiny of 50.54 notifications (escalating the review process, RAIs)
  - Licensee solicitation of NRC approval of 50.54(p) changes
  - Licensee fear of license amendment process
    - Perception that applying for license amendment = decrease in effectiveness
    - Fear of potential hearing on the amendment request

Slide 18: ISFSI Security
Jason Zorn

- Current regulations in Part 73 contain inconsistencies for ISFSI security
  - General vs. specific treated differently with regard to applicability of DBT
  - DBT rule contains conflicting language
  - Rule applicability for generally-licensed and specifically-licensed collocated ISFSIs is not clear
  - Commission policy for ISFSI protection strategy not clearly set forth
- NRC began issuing orders to ISFSIs in 2002 to require enhanced security measures. Orders maintained "status quo" for disparities in regulations
- In 2007, policy paper to Commission (SECY-07-0148), staff sought direction on several policy issues prior to initiating rulemaking. Commission gave following direction:
  - Staff should commence rulemaking to revised ISFSI regulations after developing technical basis
  - Technical basis should be distributed for stakeholder feedback
  - Rule should apply a dose-based, performance-based limitation (detect and assess), rather than a requirement to protect against the DBT (denial)

- Technical basis published for comment on regulations.gov on December 16, 2009. Comment period closed on January 31, 2010.
- Staff has received significant stakeholder comments that universally seem to oppose the new direction. Staff is currently developing another policy paper for the Commission.

~~OFFICIAL USE ONLY – ATTORNEY/CLIENT PRIVILEGE~~

Slide 19: Security During New Reactor Construction
Jason Zorn

- Staff had recommended security assessment rulemaking in 2006 (SECY-06-0204)
  - Rule would have required designers and applicants to assess security features that would be incorporated into the facility design
  - Commission disapproved rulemaking and directed staff to pursue aircraft impact assessment rulemaking
- Industry had voluntarily begun efforts to develop generic construction security requirements; based on industrial security model (protection of assets)
- Staff recommended a rulemaking in 2007 (SECY-07-0211)
  - Though some NSIR staff wanted ton include fingerprinting as part of the requirements, the paper did not recommend that, but recommended leaving it open as an option.
  - Commission approved rulemaking and directed staff to leave fingerprinting issue "open, as a last resort, if alternative measures cannot be developed."
  - Staff was directed to solicit public comment on fingerprinting issue
- Draft proposed rule was published on regulations.gov for public comment in March 2010.
- Proposed rule likely to be delivered to Commission in Fall 2010

Current and Future Issues in Security
OGC Security Seminar – Part II
April 7, 2010

Zorn Speaker Notes

Slide 6: Cyber Security

- Development of Cyber Security Rule
  - 2002 ICM Order:
    - reference to cyber
    - licensees only required to assess vulnerabilities
  - 2003 DBT Order
    - reference to cyber in context of insider threat
  - NEI 04-04
    - Voluntary industry initiative for uniform cyber protection standards
    - Limited in scope; Assessment but no protection
    - Not tied to any regulatory requirement; unenforceable
  - 2006 Proposed Power Rector Security Rulemaking
    - Proposed 73.55(m): protection of digital equipment and systems
  - 2007 Final DBT Rule
    - Included "cyber attack" as element of the DBT
    - Not included in the 2005 proposed rule
    - Required to be "considered' in EPAct 2005
  - 2009 Final Power Reactor Security Rule
    - "Cyber Security Rule": 73.54
    - Separate section of the regulation to accommodate other classes of licensees (currently only applied to power reactors)
    - Broad, programmatic requirements
  - Regulatory Guide 5.71
  - Industry Guidance (NEI 08-09)

- Scope of the Rule
  - Scope of rule limited by application of Part 73 security requirements
  - Part 73 focused on "radiological sabotage" for reactors (significant core damage)
  - Rule only applies to equipment that, if comprised could directly or indirectly result in radiological sabotage
  - Does not include equipment without potential for radiological sabotage, even if the equipment is subject to safety regulations

- Cyber Security Plans
  - Required to be submitted by operating reactors NLT November 23, 2009
  - New reactors required to amend application after effective date
  - Cyber Security plan one of 4 plans required by 50.54; part of license
  - NRC and industry separately developed generic templates
    - Mix of who is using what so far

Staff is currently performing acceptance review for cyber security plan submittals
- Submittals used a variety of templates

- Some based on NEI versions that the staff had not endorsed; resulted in significant numbers of RAIs
- Staff working with industry to resolve RAIs either generically or on a site by site basis
- Implementation schedule
  - No time specified in the rule
  - Staff late in developing guidance on what an acceptable schedule is

- New Reactors
- other licenses

- Interaction with FERC/NERC — ERO / EPAct
  - Relationship between FERC and NERC/what is NERC?
  - FERC Critical Infrastructure Protection Order
    - Nuclear exemption — all NPP Facilities
    - Revision; NRC and industry comments — NRC: too broad
    - Publication of revision — vary depends what "balance of plant"
      - Exemption process for equipment under NRC cyber requirements
  - Memorandum of Understanding
    - MOU with NERC (as opposed to FERC)
    - Attempts to mitigate dual regulation, conflict, etc.
    - Describes authorities of NRC and NERC
    - Describes exemption process and coordination role
    - Unable to include reimbursement clause for NRC to conduct inspections on behalf of NERC (Economy Act restrictions)

Slide 16: Force-on-Force Exercises

- EPAct 2005 (Section 651) mandated that NRC conduct "security evaluations" at least every 3 years at Commission-designated facilities.
- Security evaluations "shall include" force-on-force" exercises
- Shall "to maximum extent practicable, simulate security threats in accordance with any design basis threat applicable to a facility."
- Requires annual report to Congress in classified and unclassified form

- Prior to 9/11, NRC had conducted force on force exercises at NPPs
- FOF includes "composite adversary team"
  - Team has capabilities consistent with the DBT
  - FOF evaluation includes 2 week assessment; 1st week walk through, tabletops, target set evaluation, etc.; 2nd week 3 FOF exercise
- CAF strategy to destroy complete target set
  - Target set is set of equipment or operator actions that, if compromised, would prevent safe shutdown of reactor

- FOF Enhancement Program
  - staff proposing changes to make the FOF program
  - Changes would take a more "holistic" approach to evaluating security
  - Go from "pass/fail" solely based on exercise results to weighing of other factors
  - Other factors include:
    - Officer training

        - Target set ID
        - Controller training and performance
    - Staff undergoing extensive evaluation, including public meetings and Congressional briefings
    - Criticisms:
        - From industry: changing the goalposts midgame (changes would make it easier to identify failures)
        - From public interest stakeholders: changes would make it easier to "cover up" failures because failure of exercise could potentially not result in overall failure
- New Reactor Force on Force
    - No requirement to complete FOF prior to operation
    - Staff is considering whether or not this is needed and how it would be imposed
    - If not prior to operation, then when? How long after is appropriate?

Slide 16: Enhanced Weapons/Firearms Background Checks

- EPAct 2005 section 653 (added section 161A)
- 4 Basic Provisions:
    - State law preemption
    - Authority for select licensees to use weapons and equipment illegal under Federal and state law (e.g. fully automatic weapons)
    - Conduct of NICS checks (Brady Bill) on all armed security officers
    - Development and issuance of "guidelines" approved by the AG
- Preemption and enhanced weapons both "voluntary"
- NICS checks mandatory
- Negotiation of guidelines with DOJ took nearly 4 years to complete. Guidelines issued in September 2009.
- Rulemaking
    - Proposed rule in October 2006 (prior to guidelines)
    - Proposed rule split from power reactor security rule in December 2008
    - Revised proposed rule to be issued soon
    - Final rule sometime early next year?

Slide 16: Remotely Operated Weapons Systems (ROWS)

- Increasing licensee interest in use of ROWS
    - Seen as a "force multiplier"
    - Reduces number of security officers
    - Reduces exposure of security officers
    - Potentially more accurate because of tracking, infrared, thermal
- Only one licensee currently using a system
- Legal and policy issues
    - Deadly force (defense of self/defense of others)
    - Safety (accurate target identification, control of malfunctions)
    - Reliable operability (harsh weather, mechanical malfunction)
    - Incorporation of "enhanced weapons"?

Slide 16: Changes to Security Plans

- Security plans (physical security, T&Q, Security contingency, cyber) part of the license per 50.54(p)
- Changes to security plans are changes to the license, thus requiring license amendment
- Except!
  - When changes do not decrease the effectiveness of the plan licensees may make changes without prior NRC approval
  - Requires notice to NRC and written description within 60 days of changes
- Common issues with plan changes:
  - Staff over-scrutiny of 50.54 notifications (escalating the review process, RAIs)
  - Licensee solicitation of NRC approval of 50.54(p) changes
  - Licensee fear of license amendment process
    - Perception that applying for license amendment = decrease in effectiveness
    - Fear of potential hearing on the amendment request

Security During New Reactor Construction

- Staff had recommended security assessment rulemaking in 2006 (SECY-06-0204)
  - Rule would have required designers and applicants to assess security features that would be incorporated into the facility design
  - Commission disapproved rulemaking and directed staff to pursue aircraft impact assessment rulemaking
- Industry had voluntarily begun efforts to develop generic construction security requirements; based on industrial security model (protection of assets)
- Staff recommended a rulemaking in 2007 (SECY-07-0211)
  - Though some NSIR staff wanted ton include fingerprinting as part of the requirements, the paper did not recommend that, but recommended leaving it open as an option.
  - Commission approved rulemaking and directed staff to leave fingerprinting issue "open, as a last resort, if alternative measures cannot be developed."
  - Staff was directed to solicit public comment on fingerprinting issue
- Draft proposed rule was published on regulations.gov for public comment in March 2010.
- Proposed rule likely to be delivered to Commission in Fall 2010

ISFSI Security

- Current regulations in Part 73 contain inconsistencies for ISFSI security
  - General vs. specific treated differently with regard to applicability of DBT
  - DBT rule contains conflicting language
  - Rule applicability for generally-licensed and specifically-licensed collocated ISFSIs is not clear
  - Commission policy for ISFSI protection strategy not clearly set forth
- NRC began issuing orders to ISFSIs in 2002 to require enhanced security measures. Orders maintained "status quo" for disparities in regulations
- In 2007, policy paper to Commission (SECY-07-0148), staff sought direction on several

policy issues prior to initiating rulemaking. Commission gave following direction:

- Staff should commence rulemaking to revised ISFSI regulations after developing technical basis
- Technical basis should be distributed for stakeholder feedback
- Rule should apply a dose-based, performance-based limitation (detect and assess), rather than a requirement to protect against the DBT (denial)

- Technical basis published for comment on regulations.gov on December 16, 2009. Comment period closed on January 31, 2010.
- Staff has received significant stakeholder comments that universally seem to oppose the new direction. Staff is currently developing another policy paper for the Commission.