Confidentiality, Security and the Desire for Open Communication in the Transport of Radioactive Material to a National Repository

A presentation to the
DOE Transportation External Coordination (TEC) Working Group Meeting
Albuquerque, NM
21-23 April 2004

Ronald B. Pope
Consultant

Objectives

- Address and prompt TEC discussion on issues of Confidentiality in RW Transport Operations – addressing questions such as:
  - Why must we be concerned?
  - How to address the DESIRE to know versus the NEED to know?
  - How to establish guidelines acceptable to all?
  - How to develop a confidentiality regime and ensure security in a complex socio/political environment?

Why must we be Concerned?

- Domestically and internationally -
  - Potential for terrorism, malicious acts, etc. are of heightened concern
  - Security requirements have been in effect for years
  - Additional efforts underway to enhance security
  - US Government is investing heavily in security

Desire versus Need to Know?

- **A. Gonzalez, Director of IAEA Division of Radiation, Transport and Waste Safety (July 2003 Transport Safety Conference):**

  While improvement in communications will also improve safety, as people who are well informed can react in a better way, it may jeopardize security.
  This is an issue of great concern, particularly after the events of 11 September 2001.
  A proper balance must be established between safety and security.
  A proper balance must be established between safety and security in relation to communication requirements.

How to Establish Guidelines?

- Existing international guidance for transport of nuclear materials [IAEA INFCIRC/225/Rev.4 (Corrected)]:
  - Consider country's design basis threat
  - Provide physical protection in depth
  - Avoid the use of regular movement schedules
  - Require predetermination of trustworthiness of involved individuals
  - Limit advance knowledge of transport information to minimum number of persons
  - Protect confidentiality of information

Confidentiality Regime to Ensure Security?

- **USE SOUND PRINCIPLES**
  - Employ sound Operational Security "OPSEC" * practices and principles
  - Recognize increased interest by, and innovativeness of, potential subversive groups
  - Recognize that malicious acts have the potential to cause damage
  - Act accordingly, be vigilant and employ sound "OPSEC" principles from outset

* e.g. – see Interagency Operational Security (OPSEC) Support Staff booklet, Glossary, Mar 96

Apply Sound OPSEC Principles

- Understand threats & vulnerabilities, determine risks, develop countermeasures, then:
  - Restrict knowledge to those that Must Know (i.e. always establish basis for Need to Know)
  - Only release information on shipments
    - to trustworthy individuals
    - to the degree necessary
    - through secure channels
    - through clear, written plans and procedures
    - consider how actions may provide people valuable information with malicious intent

Applying Sound Principles…

- **In developing security plan requirements for training of HazMat shippers,, in response to the statement that "*It is critical that the carrier and shipper plans remain confidential, not subject to public disclosure and Freedom of Information Act requests*", the DOT noted that it "…*will not collect or retain security plans*." DOT noted it would only evaluate them during a compliance inspection.**

Fed. Reg. 68/57, March 25, 2003

Applying Sound Principles...

- NRC guidance on physical protection for irradiated fuel in transport (10 CFR 73.37) includes requirements for
  - A communications center continuously staffed
  - Making arrangements with local law enforcement agencies along routes
  - Notification to governor or governor's designee
  - Specification of information provided to state designee
  - Requirement that information is protected by state until 10-days after shipment has entered the state

Conclusions

- In today's environment – certain security-related information must be protected
- A sound confidentiality regime must be developed
  - DOE
  - contractors
  - stakeholders
- Multiple requirements and guidelines available
  - internationally (IAEA, IMO, UNECE, etc.)
  - domestically (DOE, NRC, DOT, etc.)
- RW expected to meet or exceed those requirements and guidelines in its activities
- RW expected to work with stakeholders to define security requirements and confidentiality regime

Conclusions ....

- Emergency response training, operational needs and Ops Sec requirements to be addressed in development of the Transportation Operations Plan
- Preparations at stakeholder level include
  - general knowledge of routes and schedules available through NEPA, etc.
  - training of potential emergency responders
- Detailed knowledge, for security purposes, only to be given to official designees
  - with a need to know
  - capable of protecting information
- Stakeholders need to work together with DOE to establish a sound confidentiality regime acceptable to all