

A Practical Approach to Assessing Nuclear Threats

22 June 2009

Dr. Patricia Holahan, Director
Division of Security Operations
Office of Nuclear Security and Incident Response
U. S. Nuclear Regulatory Commission

Introduction



- Need for a consistent and transparent approach to assessing nuclear threats
- Process needs to already be in place
- Requires multi-disciplined team approach
- Ensures assessment is timely and effective

The Information Assessment Team

- Focal point for assessing all reported threats
 - **A threat is defined as information - explicit or implied that a malevolent act may be committed**
- Available 24/7 through NRC Operations Center
- Consists of threat analysts, security specialists, and reactor, materials and cyber technical experts
- Coordinates outreach to licensees, law enforcement and other government agencies, including Intelligence Community
- Provides recommendations for follow-on actions

Handbook of Potential Scenarios

- Handbook developed to facilitate discussions and guide potential actions

- General categories of scenarios include
 - Suspected tampering, vandalism, sabotage

 - Suspected or actual intrusion

 - Nuclear extortion threat

 - Suspected theft of Special Nuclear Material

 - Bomb threat

Handbook of Potential Scenarios

- General categories of scenarios include
 - Suspected Arson
 - Radiological Dispersal Device Threat
 - Radioactive Contamination threat
 - Non-specific threats
 - Computer System or cyber threat

Handbook of Potential Scenarios



- Initial assessment evaluates from safety, operational, security and investigative perspective
- Goal to identify any immediate threat to safe operation
- Identify underlying security issues
- Primary responsibilities for response belong to licensee and law enforcement
- NRC provides oversight of licensee actions

Database Development



- Post 9/11 password-protected database developed to record actions regarding threats and security events
- Available to licensees and appropriate government agencies
- Used for development of trend reports
- Feeds into National-level evaluations of threats to all elements of critical infrastructure

Conclusion

- IAT process has proven to be an effective process for quickly assessing threats
- Can be adapted to other countries' regulatory, legal and organizational structure as well as other types of critical infrastructure
- Key element is having process in place
- Should have small group of experts available 24/7
- Look at safety as well as security concerns
- Enhances information-sharing between regulatory authority and other key elements of government

Contact Information:

Dr. Patricia Holahan, Director
Division of Security Operations
Office of Nuclear Security and Incident Response
U. S. Nuclear Regulatory Commission
Patricia.Holahan@nrc.gov