International Regulators Conference on Nuclear Security
DECEMBER 4-6, 2012
HILTON HOTEL • ROCKVILLE • MARYLAND

The Design Basis Threat (DBT) and Threat Assessment

Michael F. Weber
Deputy Executive Director for Materials, Waste, Research, State, Tribal and Compliance Programs

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

Core Tenets of Nuclear Security

• **Identify and Define**: Nuclear target sets for protection from external and internal adversaries. High correlation between consequence and protection level. (IAEA *INFCIRC/225/Rev5, NSS No. 10 DBT Development*)

• **Assess Threat**: Which adversaries have the malevolent intent, opportunity, and capability to compromise nuclear target sets – and how.

- Screen all sources for intent, capability, & opportunity,
- Translate threat intelligence into adversary attributes,
- Modify adversary attributes based dynamic threat environment and subject to policy considerations. (*NSS No.10 DBT Development)*

• **Develop, Test & Refine**: Physical and cyber protective strategies are developed, exercises implemented to test strategies, and additional security measures implemented, if necessary.

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

NRC Design Basis Threat Process

• Consistent with IAEA Guidelines, the NRC continuously assesses, updates, and modifies its DBT through a five-step process:

- Review threat intelligence,
- Assess adversary capabilities, attack patterns, location of attacks,
- Task Intelligence/Law Enforcement Communities for additional information on adversary tactics, techniques, and procedures,
- Conduct technical analysis of the integrated effectiveness of existing Member State, regional, local response measures, and
- Engage stakeholders – including operators – as appropriate

Key Questions

• How do national authorities incorporate the dynamic cyber threat into DBT procedures?

• DBTs are “risk-informed” and threat is one element of risk. How are vulnerabilities and potential consequences considered in DBT procedures?

• DBTs contain sensitive or classified information. How do national authorities balance information protection with the need to share information with operators and other security organizations?

• In establishing DBTs, is there a point at which societal costs become excessive in protecting against low probability, high consequence events?