Contribution ID: **217** Type: **Interactive Content Presentation**

# Cyber Security Considerations for Implementing the Design Basis Threat at Nuclear Facilities

Cybersecurity threats continue to grow, and the nuclear sector recognizes that it must have compensating measures in place to address these threats. The evolution of cyber threats to critical systems is growing at an alarming rate and it is important that the nuclear community response accordingly. One mechanism to addresses the cyber threat is through development and utilization of a Design Basis Threat (DBT). Historically the DBT was originated as a key element in a toolset enabling an Operator to gain a physical security perspective based on understanding the capabilities of an adversary to cause acts of radiological sabotage or the theft of special nuclear materials.

The DBT enables the Operator to implement a baseline protective strategy required by the State. The DBT outlines the threat adversary's capabilities. Motivations and Opportunities are further informed by the Intelligence Partners, and the Operator's Defensive Strategy and Posture. This guidance allows the Operator to develop the necessary site security plan and protection systems to meet the DBT requirements.

The purpose of this paper is to outline how cyber security DBT considerations can impact the physical security protective strategy and provide a methodology for operators and competent authorities to utilize to ensure that the DBT is integrated into the cyber mitigation strategies both from the cyber-physical perspective as well as the physical-cyber perspective. The dynamic nature of the threat based on day-to-day changes that occur in cyber security –vulnerability discovery and mitigations - directly affects the DBT model review and update cycle by the CA and Operator evaluation and implementation.

A nuclear security framework that supports the DBT requirements as well as the security challenges must be considered within the site-specific nuclear security plan that is approved by the component authority. The approach will very state to state, from very prescriptive measures to simple self-directed security implementations subject to an occasional compliance-based assessment. Therefore, this paper will evaluate the cybersecurity challenges associated with creating, managing and utilizing a DBT by examining the physical and cybersecurity protective measures developed through a risk-based assessment process, within the context of what is required by the competent authority to promulgate and support the Operator's appropriate protection profile to prevent the theft or sabotage of nuclear materials.

## State

United States

## Gender

Male

**Authors:** RODRIGUEZ, Julio (Idaho National Laboratory); Mr KNIGHT, Jeffrey (Idaho National Laboratory)

**Presenter:** RODRIGUEZ, Julio (Idaho National Laboratory)

**Track Classification:** CC: Information and computer security considerations for nuclear security