U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Philip A Craig Jr / Jeff Dagle

Pacific Northwest National Laboratory

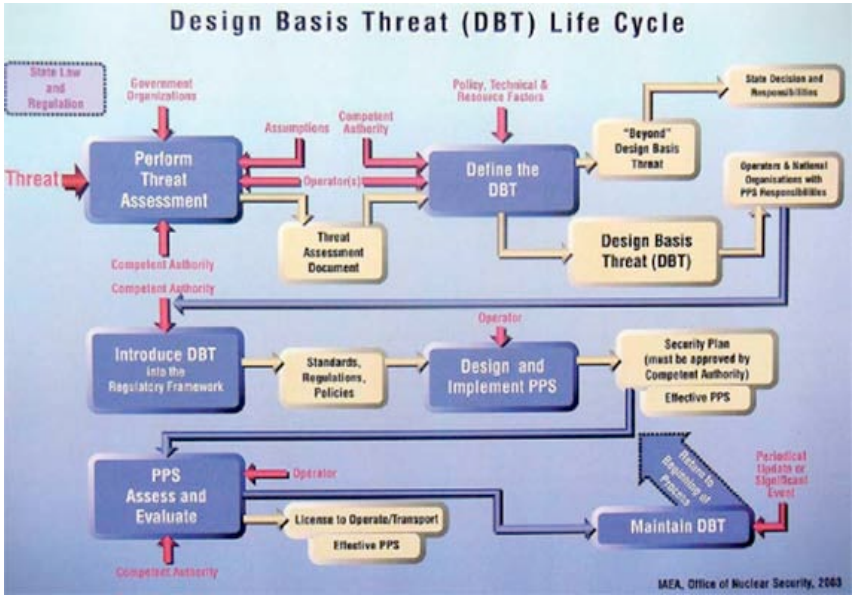
"Implications of Design Basis Threat on Critical Infrastructure and Homeland Security"

Note!

- The context of this presentation doe *not* represent any findings that are classified or non-classified
- The notion or discussion of a critical infrastructure DBT is not itself *sensitive* and no details that would present such sensitivities are represented in any way in this presentation

Summary Slide: Design Basis Threat Implications

- **Outcomes:** Implications of Design Basis Threat concepts relevant to energy sector critical assets and threat
- **Roadmap Challenge:** Vendors do not have specific requirements or standards to build to: threats are hard to demonstrate and quantify
- **Major Successes:** Major projects in work to set an unprecedented knowledge of critical infrastructure threat. Internal PNNL funding augmenting mission space ($127K, +$250K FY11/12)



- **Schedule:** No scheduled key deliverables completed
- **Level of Effort:** $100K
- **Funds Remaining:** $95K
- **Performers:** PNNL
- **Partners:** SNL (TBD)

Technical Approach and Feasibility

- **Approach**
  - Examine the implications of design basis threat (DBT) selection and threat modeling on security policies, procedures, and practices for critical infrastructure.
  - Identify any new key elements needed for cybersecurity.
  - Integrate cybersecurity and physical security methodologies focusing on type, composition, and capabilities of adversary characteristics to formulate credible threat/adversary scenarios.
  - Develop DBT framework providing mitigation measures and response strategies that significantly reduce or eliminate adverse impacts to critical infrastructure.

Technical Approach and Feasibility

- **Metrics for Success**
  - Include successful physical security DBT attributes in initial evaluation.
  - Ensure a critical infrastructure DBT framework is adaptable to *identified* and *postulated* risk.
  - Provide a *integrated* physical/cyber DBT approach to ensure defensive strategies provide a comprehensive and coordinated response to an adversary and threat.

Technical Approach and Feasibility

- **Challenges to Success**
  - Physical security is often *segregated* from cybersecurity
    - Leverage internally funded PNNL programs/projects to maximize physical/cyber DBT integration
  - Cybersecurity has a very different and dynamic threat landscape and adversary characteristics
    - Leverage inter-laboratory threat and adversary work in additional to PNNL's research an knowledge to ensure threat/adversary profiles are current.

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Established relationship with SNL researchers to integrate physical/cyber threat assessment efforts.
  - Tracking and interfacing with internal PNNL research projects to ensure DOE-OE deliverable is focused on the ability to assess and evaluate an overall defensive security postures' mitigation/response capability.

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - What do you need (e.g., expertise, action, resources) from industry?
    - Proactive, productive, and pragmatic progress in implementing cyber security.
    - Influential engagement (BPA? TVA?)
  - What will you do/have you done to gain industry input and assistance?
    - PNNL will continue to champion the DBT framework concept based on depth and experience in that domain.
    - Continue current engagement with FERC to provide recommendations in the regulatory space.
  - What are the challenges to gaining this input?
    - Industry is unregulated from this perspective. NERC and FERC both have not provided tangible direction. Industry is "complying" to their best ability in some cases and resisting the process in many others.

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Who will use the technology or knowledge? How will they apply it? How should they not apply it?
  - What are your plans to gain industry acceptance?
  - How does this solution fit into the existing paradigm of power systems technologies? How does it leverage (and avoid interference with) existing capability to protect the reliability of power systems?

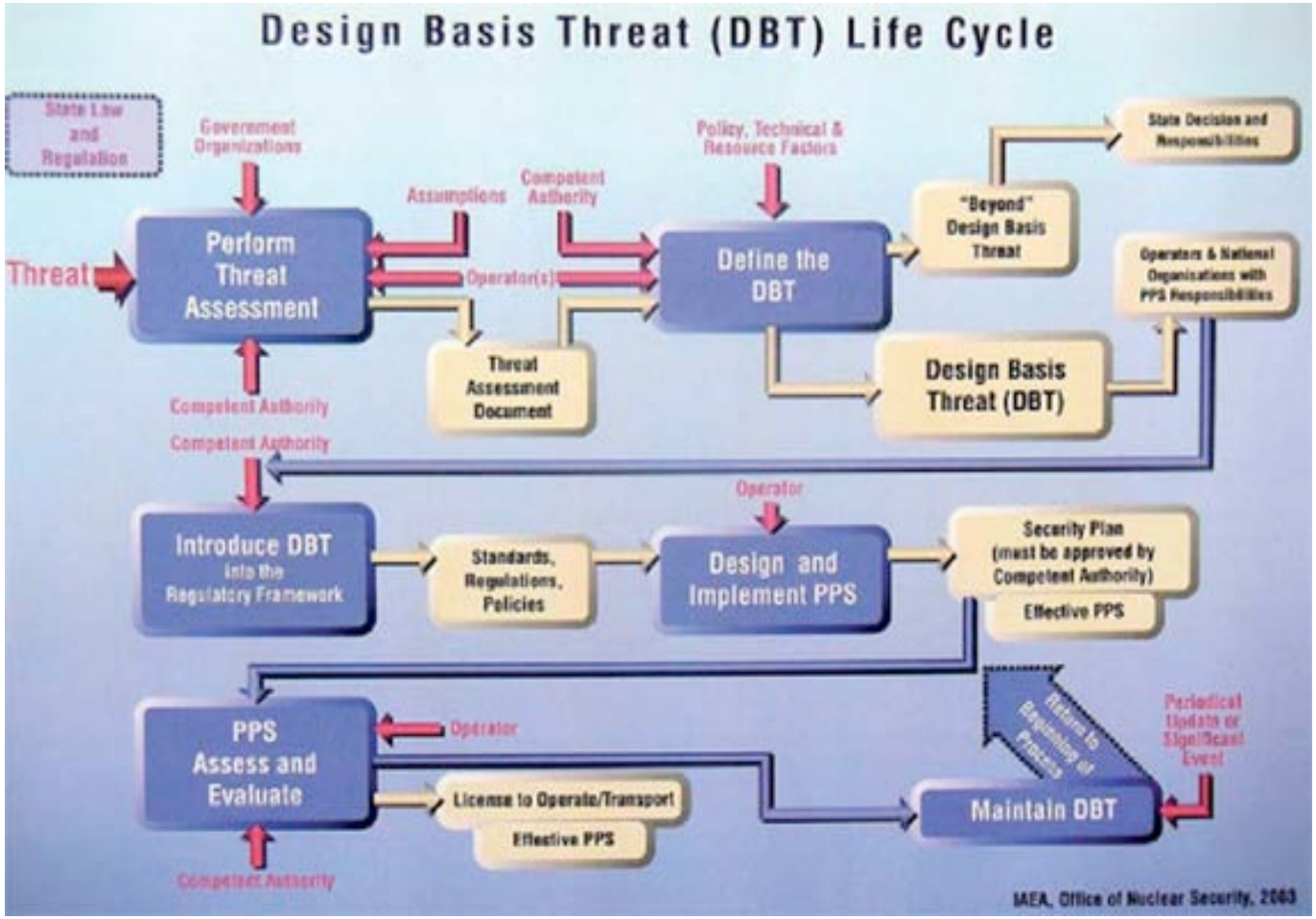
Next Steps

- **Approach For the Next Year**
  - Adjust current milestones to align with related DBT activities to ensure the proposed DBT framework that is delivered to DOE-OE is fully enabled by current assessment data
  - Risks are minimal as the proposed DBT framework that would be utilized for critical energy infrastructure is primarily challenged by policy making and cost. A framework validated by assessments is essential in mitigating both

Next Steps

- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - This CEDS task will offer significant value to all DHS sector identified critical infrastructure and hopefully form a consistent DOE/DHS message to industry
- **Describe potential follow-on work, if any**
  - Development of scenarios that identify blended critical infrastructure threat (e.g. A simultaneous attack that would offer heightened challenge and greater impact by attacking multiple and different infrastructure)
  - Cost (TBD) …*work may need to be performed in more sensitive space*.

Established DBT Lifecycle



QUESTIONS?

Philip A Craig Jr.

PNNL

509-375-4464