DEFENSE IN DEPTH
A SECURITY PERSPECTIVE

Richard L. Donovan
Department of Energy
Office of Enterprise Assessments

Defense in Depth? – It's Fundamental

- **As defined in the DOE S&S Policy Information Resource[1]**
  - **The use of multiple, independent protection elements combined in layers so that system capabilities do not depend on a single component to maintain effective protection against defined threats.**

[1] DOE Policy Information Resource, (https://pir.doe.gov/)

Defense in Depth? – It's Fundamental

- **The concept of DID as applied in security systems is similar that for safety systems. As with safety, the following must be addressed by security systems:**
  - **Inadvertent breach of a barrier,**
  - **Deliberate, but not malicious, breach of a barrier (e.g., under time pressures),**
  - **Unanticipated equipment failure,**
  - **Acts of God – e.g., fire, earthquake or flood, and**
  - **Accidents etc.**

Defense in Depth? – It's Fundamental

- **Security DID must consider another aspect – the deliberate, malicious challenge to the security system**
  - **Adaptive behavior – intelligent response to security elements, unanticipated tactics and strategy, etc.**
  - **Malicious acts may have greater consequences, for example:**
    - **Accidental vs. assisted (e.g., by explosives) release of radioactive material and/or radioactive materials taken to a populated area before release.**
- **Likelihood of attack is unknowable**

Need, Objective and Scope of DID

- **Any security element in isolation can be defeated by a determined adversary.**
  - **Uncertainty in methods of attack make multiple layers of defense necessary to achieve high assurance of protection effectiveness.**
  - **Further, within a layer, complimentary technologies/measures are necessary to provide high assurance of protection effectiveness.**
- **DOE applies DID to all protected assets, with effectiveness scaled to consequence.**

Implementation Approach

- **Assume that a determined effort will be made to defeat the system.**
- **Require effectiveness in all weather conditions.**
- **Realize that operations must continue in spite of security requirements.**
- **Establish general requirements by asset type and quantity but provide freedom to customize to site requirements.**
- **Safety and security may both derive benefits from some measures.**

Sufficiency/Adequacy/Risk Analysis

- **Since the likelihood of attack is unknowable, a deterministic evaluation of risk is not possible.**
- **DOE creates a design basis threat (DBT) that describes threat characteristics and capabilities.**
- **Consequences are addressed by different levels of threat within the DBT.**
- **DOE system adequacy is defined as a certain (classified) expected level of success against the DBT adversary.**

Sufficiency/Adequacy/Risk Analysis

- For high consequence targets (high level threats in the DBT), the DOE uses computer models, FoF performance tests, and other methods to establish likely performance.
- For lower consequence targets, DOE establishes a required DID implementation within DOE policy.
- For lower consequence targets, DOE may use qualitative analyses to determine effectiveness of protection.

Summary

- **The principles of DID have informed DOE security directives.**
- **The adequacy of the implementation of DID principles can be measured by analyses and performance testing.**
- **When considering intelligent, adaptive challenges, conditional risk (probabilities of success given a malevolent challenge) is the appropriate metric.**

DOE's Official Position on DID

- **DOE Directives incorporating DID**
  - **DOE Order 470.3B, Graded Security Protection (GSP) Policy**
  - **DOE Order 470.4B, Safeguards and Security Program**
  - **DOE Order 471.6, Information Security**
  - **DOE Order 473.3, Protection Program Operations**
  - **DOE Order 474.2, Nuclear Material Control and Accountability**

DOE's Official Position on DID

- **DOE technical guidance incorporating DID**
  - ***Vulnerability Assessment Standard*** **(DOE-STD-1192-2010)**
  - ***Nuclear Material Control and Accountability Standard*** **(DOE-STD-1194-2011)**
  - ***Protection Program Defensive Planning For Fixed Facilities Standard*** **(DOE STD-1207-2012)**
- **On-line resources**
  - **Current DOE Directives (https://directives.doe.gov/)**
  - **Current DOE Technical Standards (Google DOE technical standards) (http://energy.gov/ehss/services/nuclear-safety/department-energy-technical-standards-program/doe-approved-technical)**
  - **S&S Policy Information Resource (https://pir.doe.gov/)**