
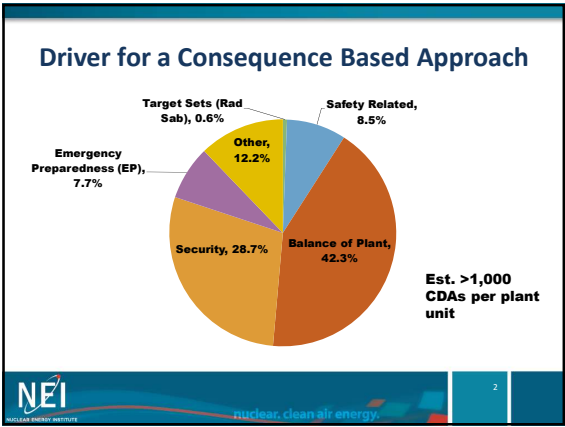


Implementing a Consequence-Based Approach to Cyber Security



William Gross
 Senior Project Manager, Engineering
 2016 Regulatory Information Conference
 March 8, 2016 • Rockville, Maryland

Draft Revision: 20160115c






A System Assessment

Consequence Approach Implementation

- Provision assets based on impact of attack
- Indirect assets
 - No direct impact to function, or
 - Consequences mitigated prior to impact.
 - Includes low impact EP and balance of plant assets
- Direct assets - those not identified as indirect
- Cyber security controls graded



Benefits and Future Applications

- Current approach working well for reactors:
 - Achieving desired outcomes (75% or more indirect)
 - Permits licensees to focus on high consequence assets
- Improvements if considered for other licensees:
 - Not all functions are equally attractive to an adversary seeking to harm the health and safety of the public
 - Prioritize only those assets that if compromised would likely result in radiological sabotage or theft of SNM
- Best - eliminate any system not directly related to preventing sabotage, theft of SNM

