
Critical Infrastructure Protection



Critical Infrastructure Protection Defined



Critical Infrastructure Protection is the process and actions to defeat or minimize an attack against America's most critical assets, and by doing so, eliminate or reduce the consequences of such acts.

....Dave Sanders

Critical Infrastructure Protection in Action



Protection
of



Becomes a
Function of



And is
Accomplished by

- **Information and digital data**
 - Confidentiality
 - Availability
 - Integrity
 - Accountability
 - Non Repudiation
- **Assets**
 - People
 - Structures
 - Equipment
- **Operations**
 - Critical Processes
 - Core Business needs
 - Safety
 - Reliability

- **Investment in**
 - People
 - Resources
 - Technology
- **Policies and Procedures**
 - Rules
 - Regulatory Guidance
 - Best Practices
- **Acquisition**
 - Strategy
 - Implementation
 - Life Cycle

- **Management**
 - Assessment
 - Policy Review
 - Policy Formulation
 - Planning
 - Training & Education
- **Protection**
 - Access Controls
 - Authentication
 - Firewalls
 - Physical
 - Gates
 - Guards
 - Fences
 - Lights
 - Other
 - Layered defense

- **Detection**
 - Intrusion Detection Devices
 - Monitoring
 - Early Warning
- **Recovery**
 - Fail-over
 - Backups
 - Continuity of Operations
- **Consequence Management**
 - Response to events
 - Resiliency
 - Reconstitution
- **Devaluation**
 - Hardening
 - Resilience
 - Significance

To Guarantee the Protection or Use of:



Protection
of



Becomes a
Function of



And is
Accomplished by

- **Information and digital data**
 - Confidentiality
 - Availability
 - Integrity
 - Accountability
 - Non Repudiation
- **Assets**
 - People
 - Structures
 - Equipment
- **Operations**
 - Critical Processes
 - Core Business needs
 - Safety
 - Reliability

- **Investment in**
 - People
 - Resources
 - Technology
- **Policies and Procedures**
 - Rules
 - Regulatory Guidance
 - Best Practices
- **Acquisition**
 - Strategy
 - Implementation
 - Life Cycle

- **Management**
 - Assessment
 - Policy Review
 - Policy Formulation
 - Planning
 - Training & Education
- **Protection**
 - Access Controls
 - Authentication
 - Firewalls
 - Physical
 - Gates
 - Guards
 - Fences
 - Lights
 - Other
 - Layered defense

- **Detection**
 - Intrusion Detection Devices
 - Monitoring
 - Early Warning
- **Recovery**
 - Fail-over
 - Backups
 - Continuity of Operations
- **Consequence Management**
 - Response to events
 - Resiliency
 - Reconstitution
- **Devaluation**
 - Hardening
 - Resilience
 - Significance

Then CIP Becomes a Function of:



Protection
of



Becomes a
Function of



And is
Accomplished by

- Information and digital data
 - Confidentiality
 - Availability
 - Integrity
 - Accountability
 - Non Repudiation
- Assets
 - People
 - Structures
 - Equipment
- Operations
 - Critical Processes
 - Core Business needs
 - Safety
 - Reliability

- Investment in
 - People
 - Resources
 - Technology
- Policies and Procedures
 - Rules
 - Regulatory Guidance
 - Best Practices
- Acquisition
 - Strategy
 - Implementation
 - Life Cycle

- Management
 - Assessment
 - Policy Review
 - Policy Formulation
 - Planning
 - Training & Education
- Protection
 - Access Controls
 - Authentication
 - Firewalls
 - Physical
 - Gates
 - Guards
 - Fences
 - Lights
 - Other
 - Layered defense

- Detection
 - Intrusion Detection Devices
 - Monitoring
 - Early Warning
- Recovery
 - Fail-over
 - Backups
 - Continuity of Operations
- Consequence Management
 - Response to events
 - Resiliency
 - Reconstitution
- Devaluation
 - Hardening
 - Resilience
 - Significance

And, it is Accomplished by:



Protection
of



Becomes a
Function of



And is
Accomplished by

- Information and digital data
 - Confidentiality
 - Availability
 - Integrity
 - Accountability
 - Non Repudiation
- Assets
 - People
 - Structures
 - Equipment
- Operations
 - Critical Processes
 - Core Business needs
 - Safety
 - Reliability

- Investment in
 - People
 - Resources
 - Technology
- Policies and Procedures
 - Rules
 - Regulatory Guidance
 - Best Practices
- Acquisition
 - Strategy
 - Implementation
 - Life Cycle

- Management
 - Assessment
 - Policy Review
 - Policy Formulation
 - Planning
 - Training & Education
- Protection
 - Access Controls
 - Authentication
 - Firewalls
 - Physical
 - Gates
 - Guards
 - Fences
 - Lights
 - Other
 - Layered defense

- Detection
 - Intrusion Detection Devices
 - Monitoring
 - Early Warning
- Recovery
 - Fail-over
 - Backups
 - Continuity of Operations
- Consequence Management
 - Response to events
 - Resiliency
 - Reconstitution
- Devaluation
 - Hardening
 - Resilience
 - Significance

Critical Infrastructure Challenges



Some Critical Infrastructure Challenges

- **Gaps in technology**
 - Lack of common IT Security features
- **Advances in technology**
 - Moving Faster than Security Skill Sets
- **Exposure to Common Vulnerabilities**
 - .rhosts, no passwords, simple passwords, no patching
- **Lack of pedigree to existing standards (across the board)**
 - What standards should be followed?
- **Compliance to cyber/physical security standards are voluntary**
 - Followed by some
 - Often self serving

Some Critical Infrastructure Challenges

- **Gaps with regulatory guidance**
 - Does not afford “National” awareness
 - Does not afford “National” resilience
- **Effective model for cost sharing does not exist**
 - Industry should lead, Government should back & oversee
- **Liability concerns are real!**
 - Stops “real” information flow
- **Sector Specific Agency Concept doesn’t seem to be working**
 - Authority, Funding, Integration?
- **“Inter-Dependency” analyses doesn’t work**
 - Everything seems dependent on everything else

Critical Infrastructure Recommendations



Some Recommendations



Government & Industry Together

- **Address Gaps and Advances in Technology (long-term)**
 - Create accountable security standards for vendors
 - Invest heavily in R&D and get to market



Some Recommendations



Government & Industry Together

- **Create firm standards that are universally applicable (short-term)**
 - Either through regulation or legislation
 - Reduce or eliminate exposures to potential vulnerabilities without affecting safety, reliability, or efficiency
 - Train and Educate

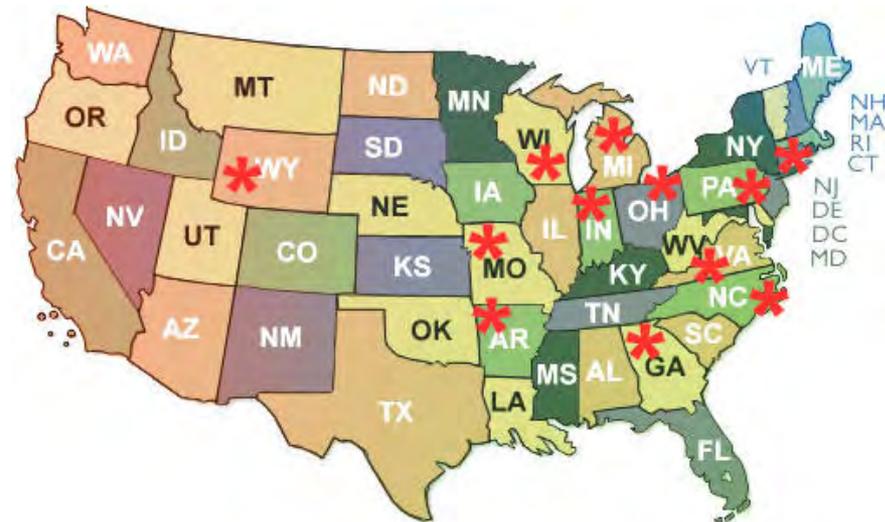


Some Recommendations



Government & Industry Together

- **Create ability for precursor and attack detection at a national level**
 - National Detection & Response Center
 - Industry Lead
 - Government Backed
 - Costs are shared
 - Jointly Operated

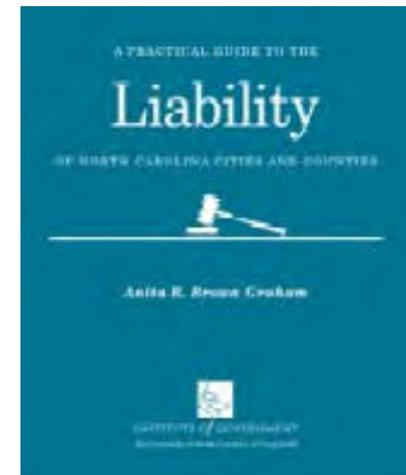


Some Recommendations



Government & Industry Together

- **Provide for Liability reform except in cases involving malicious intent**
 - **Mandatory sharing of attack details**
 - **Protection of source**
 - **Mandatory sharing of threat information**
 - **Guaranteed relief from liability for exercising “Duty of Care”**

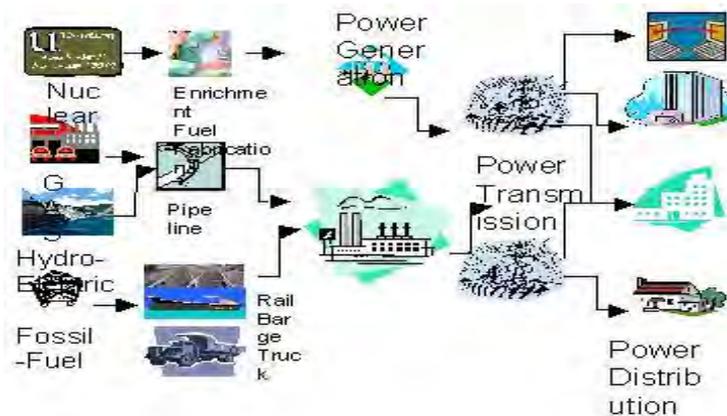


Some Recommendations



Government & Industry Together

- **Create value chains by sector to identify single points of failure**
 - Look for critical nodes
 - Look for points of failure
 - Secure them.

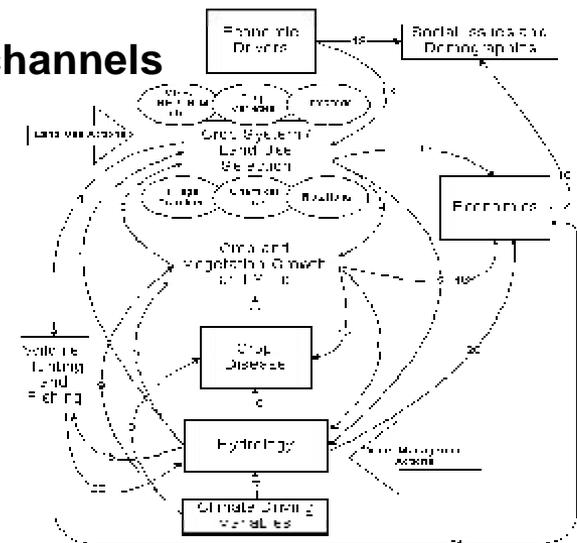


Some Recommendations



Government & Industry Together

- **Create, by sector, national resiliency plans for guaranteed continuity of operations**
 - **Address functions that preserve, extend, or protect life, liberty, and the economy**
 - **Devalue targets through hardening and duplication**
 - **Guarantee continuity**
 - **Allocate critical infrastructure communications channels**
 - **Clearly define roles and responsibilities**
 - **Exercise often.**

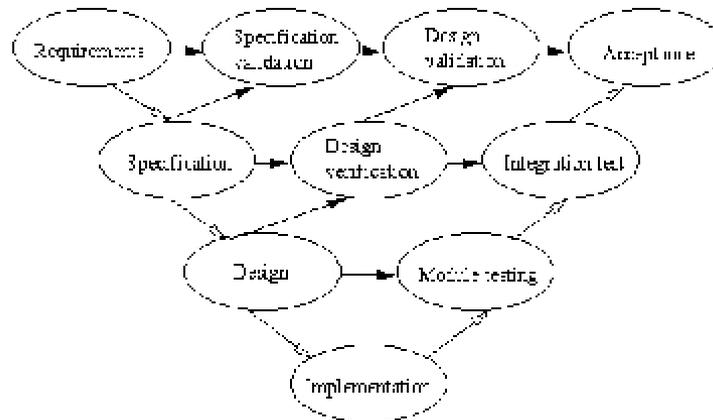


Some Recommendations



Government & Industry Together

- **Blending of government/industry roles (Cooperation)**
 - Triangle between DHS, regulatory, and industry players
 - Ability to enforce compliance through self and third party assessments
 - Third Party knowledge not associated with sector for those with no regulatory head
 - Increased intelligence capabilities within borders with judicial approval



Some Recommendations



Government & Industry Together

- **Hold industry accountable for lack of diligence in meeting minimum standards**
 - “Duty of Care” regulation
 - Take safety and reliability into consideration with security
 - Create minimum baseline for protection
 - Use third party assessments

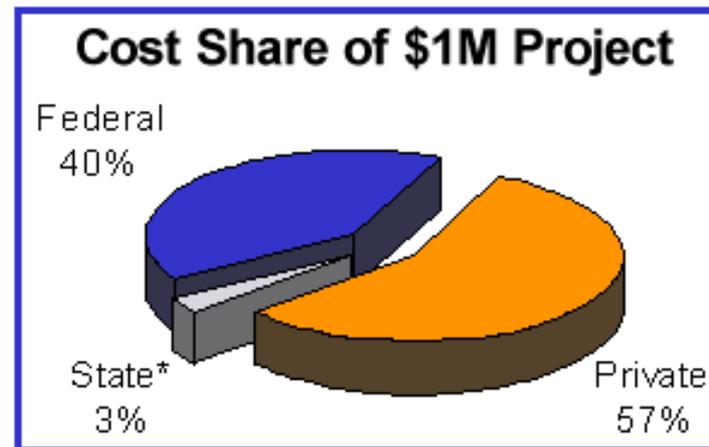


Some Recommendations



Government & Industry Together

- **Government must cost share with industry**
 - Look at life-cycle replacement rather than “all at once”
 - Back new technologies with cost savings to “Critical Infrastructure”



Questions



Thank You



Business and Systems Aligned. Business Empowered.™