Outpacing Cyber Threats:
Cybersecurity at Nuclear Facilities

March 16, 2017

Page O. Stoutland, Ph.D.
Vice President
Scientific and Technical Affairs

Cyber attacks can compromise nuclear security in several ways

Theft	Sabotage	Nuclear Weapons Systems	Data Integrity
			
Physical Protection, Control & Accounting	Safety & Operations	Communications & Control	Databases & Design Information

NTI BUILDING A SAFER WORLD

2016 NTI Index included cybersecurity

- Is cybersecurity required at nuclear facilities?
- Must critical digital assets be protected?
- Must cyber threat be included in overall threat assessment?
- Is cybersecurity assessed in a performance-based program?

NTI BUILDING A SAFER WORLD 3

NTI Index found serious cybersecurity shortfalls

NTI BUILDING A SAFER WORLD 4

NTI Cyber-Nuclear Priorities Project

- Landscape
  - Potentially catastrophic consequences
  - Increasing threat and digitization
  - Existing approaches are not effective against determined adversaries
  - Global problem
- Identify the key elements of a new cyber-nuclear strategy
  - Forward-looking
  - Scalable
  - Less constrained

NTI BUILDING A SAFER WORLD

Cyber-Nuclear Priorities

- Institutionalize Cybersecurity
- Mount an Active Defense
- Reduce Complexity
- Pursue Transformation

NTI BUILDING A SAFER WORLD

Institutionalize cyber-nuclear security

- Embed cybersecurity in the daily operations of nuclear facilities
  - People and organizational culture
  - Design solutions
  - Facility processes and practices

NTI BUILDING A SAFER WORLD

Mount an active cyber defense

- Active defense to detect and disrupt cyber intrusions as they happen
  - Access to needed technical skills
  - Characterize systems
  - Detect hackers
  - Eliminate them

NTI BUILDING A SAFER WORLD

Reduce complexity

- Complexity is the enemy of security, leading to unknown functionalities and higher levels of “noise” on the network
- Reduce complexity
  - Systems and networks
  - Individual components

NTI BUILDING A SAFER WORLD

Pursue transformation

- Develop new approaches for cyber-physical systems
  - Trustworthy and defendable systems
  - Models to simulate behavior of complex cyber-physical systems
  - 21st century non-digital systems

NTI BUILDING A SAFER WORLD

Cyber-Nuclear Priorities

- Institutionalize Cybersecurity
- Mount an Active Defense
- Reduce Complexity
- Pursue Transformation

NTI BUILDING A SAFER WORLD

Q&A

Visit:
www.nti.org
www.ntiindex.org

Follow:
@NTI_WMD

NTI BUILDING A SAFER WORLD

Backup Slides

Taking action: Institutionalize Cybersecurity

Taking action: Mount an Active Defense

Taking action: Reduce Complexity

	STAKEHOLDERS		
	Governments and Regulators	Nuclear Industry	International Organizations
Reduce Complexity	• Provide financial, personnel, and research support to efforts to minimize complexity in critical facility systems	• Characterize facility systems and networks and understand device functionalities • Demand more secure, less complex products from vendors	• Provide platforms for discussing and developing solutions for reducing complexity

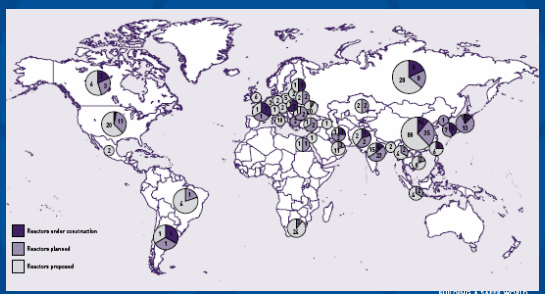
NTI
BUILDING A SAFER WORLD

Taking action: Pursue transformation

	STAKEHOLDERS		
	Governments and Regulators	Nuclear Industry	International Organizations
Pursue Transformation	• Invest in augmenting human capacity, research, and development in the cyber-nuclear space	• Support the cybersecurity efforts of relevant organizations in an effort to continue international dialogue and contribute to key research and development	• Foster innovation and continue to think creatively about how to mitigate this threat • Enlist a variety of voices and perspectives to join the conversation

NTI
BUILDING A SAFER WORLD

Nuclear reactors planned, proposed, and under construction



Cybersecurity indicators in the 2016 NTI Index

2.6 Cybersecurity	Nuclear materials and facilities are vulnerable to cyber attacks as well as physical attacks. Therefore, cybersecurity is a critical component to protecting against theft.	
2.6.1Mandatory cybersecurity	Requiring nuclear facilities to have protection from a cyber attack increases the likelihood that nuclear facilities will take measures to protect against cyber attacks.	**Do domestic laws, regulations, or licensing requirements require nuclear facilities to have protection from a cyber attack?** - No or information not publicly available - Yes
2.6.2 Critical digital asset protection	Requiring protection of critical digital assets against cyber attacks decreases the chance that an attacker can circumvent physical protection, control and accounting, and safety systems.	**Do domestic laws, regulations, or licensing requirements require nuclear facilities to protect critical digital assets from cyber attack?** -No or information not publicly available -Yes
2.6.3 Cybersecurity DBT	Requiring that the Design Basis Threat take into account the potential for cyber attacks increases the likelihood that nuclear facilities will consider cyber attacks when designing their security plans.	**Does the state consider cyber threats in its threat assessment or Design Basis Threat (DBT) for nuclear facilities?** -No or information not publicly available -Yes
2.6.4 Cybersecurity assessments	Required demonstration of performance, along with tests and assessments, improves effectiveness of and identifies weaknesses in cybersecurity measures.	**Does the regulator require a performance-based program, which includes tests and assessments of cybersecurity at nuclear facilities?** -No or information not publicly available -Yes