Remarks by Dr. Massoud Amin at the MN Senate on 9 March 2017

Madam Chair, Distinguished Senators, panelists and MN Senate Staff. Good afternoon I am honored to provide my remark in full support of the proposed bill on creation of a Cybersecurity Commission.

As we know, the security challenges of protecting human safety and the critical infrastructure in the United States and throughout the World have been highlighted during the last few decades. Worldwide cyber attacks are on the rise with evolving spectra of threats and more sophisticated adversaries – for more details please see the enclosed exhibits – in summary:

1. **First, cyber-related risk is significant:**
   a. The threat is real
   b. The Vulnerabilities are widespread
   c. And the Consequences can be disastrous

   Cybersecurity threats represent one of the most serious national security, public safety and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy… our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

2. **Second, the challenges abound:**
   a. Telecommunications and information processing (our) systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation,
   b. And the technology to exploit these electronic systems is widespread and is used extensively.

3. **Various groups and committees that have studies cyber challenges** - All seem to agree that a comprehensive and coordinated approach must be taken to protect the government's local-national security telecommunications and information systems (national security systems) against current and projected threats and that a comprehensive and coordinated approach is needed!

Increased emphasis at the state and federal level are combined with heightened needs for more innovative and better ways to enable and protect economic growth as well as secure our nation and the world while preserving individual privacies, our values, and our way of life.

I recently asked a class in our Master of Science in Security Technologies at the University of Minnesota to identify the top 5 Cyber security related issues? The feedback covered the full spectrum from malware to threats from China.

It included:

- Mobile device malware
- Government Breaches and Hacked Firewalls-
- Cloud Computing Security Related issues-
- Financial & Ecommerce-
- Healthcare Information-
- Custom Targeted Malware Attacks
- Social Engineering Attacks
- Wireless and Wireless Device Security

- Threats from China & Russia
- Advanced Persistent Threats (APTs)
- Application vulnerabilities
- Website/Internet vulnerability
- Unpatched software
- Lack of education in Cyber security
- Lack of intrusion Detection Systems
- The human factor….
- Stealing Intellectual Data
- And, Privacy concerns when the web is such a public place.

BOTTOM LINE: The RISK is significant and issues abound – unfortunately funding for our local/State's Cybersecurity protection and for the CISO office have been lacking. Creation of this Commission provides a home for in-depth discussion on these and related critical issues.

Economic growth: Security has been one of the fastest-growing professional careers worldwide, and for nearly a decade the security industry in the U.S. is a $100 billion a year business and growing.

The Homeland Security Research Corporation published a report in 2008 ranking Information Technology as the 2nd leading homeland security industry market sector with over $40 billion dollars in volume, with RFID based systems as one of the fastest growing. The U.S. government and companies will need about 60,000 cyber security professionals in the next 3 years.

These staggering numbers cut across the private sector, with a forecast of procuring over $25 billion in security service products, to government markets, forecasted to procure a cumulative $23 billion in goods and services. What does this mean? It implies a wealth of future business opportunities AND protecting our nation's security.

The Noble prized economist Professor Robert Solow at MIT quantitatively showed the power of engineering and technology in the economy—"Technology (any application of science) drives over 60% of US economy."

The future of our national security technologies, job creation, and companies' global leadership and competitiveness fundamentally depends on human capital, their abilities and innovation.

What are we doing the UofM? Minnesota has had a long distinguished history of pioneering and pivotal contributions to this, and with an endowment from the Honeywell Foundation, TLI was born twenty seven years ago at the University of Minnesota for just this reason - to develop leadership for fast-tracked professionals in tech-intensive sectors of our economy.

As an interdisciplinary center, TLI brings together 7 distinguished university endowed chairs who are at TLI, and 64 world-class faculty members from across 9 colleges and 3 centers at the University as well as top-notch executives from industry and government to serve this mission. The interdisciplinary nature and unique offerings of TLI could not be realized within the University's regular structure. TLI proactively plans collaborative and industry-responsive educational programs, research and consulting projects that leverage expertise in industry, government, and academia. TLI cuts across departmental and college boundaries to bring together over 60 senior faculty members from the College of Science and Engineering, Carlson School of Management, the Humphrey School of Public Affairs, the School of Public Health, the Law School, the Medical School and the Colleges of Food, Agricultural and Natural Resource Sciences, Veterinary Medicine, Pharmacy, and Biological Sciences.

At TLI we are working on core technologies and capabilities to strategically enhance security, quality of life and serve our society in Minnesota and beyond through our education, research, and outreach. For a timely article on "Why Cybersecurity Funding is Critical to the State of Minnesota," by my colleague Mr. Michael Johnson (whose bio is included in the folder) please see: https://tli.umn.edu/tli-blog/why-cybersecurity-funding-critical-state-minnesota

Nearly all of TLI's 1300+ M.S. recipients and 1250+ alumni of short courses are currently working in over 400 Minnesota corporations and organizations.

The impact of TLI alumni, as measured in comprehensive surveys, is outstanding in all aspects of our state's technology-intensive sectors, including electronics, defense, chemical, industrial equipment, instruments or medical equipment, information, services, food, critical infrastructure and transportation. As an example, among the 624 MOT alumni, over 33.6% have become executives and an additional 52%-54% assume senior management roles within 5-7 years after graduation.

The Institute serves as a proven internationally distinguished source for training, research and consulting in security. The U.S. Department of Homeland Security initiated a partnership with our Master of Science in Security Technologies (MSST) program for an event on cyber security in Minnesota last month, and TLI works closely with the U.S. DHS and the Naval Postgraduate School on security curriculum. We welcome our continued collaborations and look forward to maintaining our place together at the forefront of securing our digital infrastructure.

With a mission to inspire and train professionals in this critical area, our educational goal, in concert with world-class expertise already available at the University, our Master of Science in Security Technologies (MSST) program is well aligned with these state, national and international priorities, looking beyond "dogs, guns, cameras and guards," toward the increased role of cyber security and science and technology in protecting our critical assets, making our nation safer, more productive, and our economy more secure.

Here is the bottom line: The threats and risks are significant, and there is every reason to believe that they will become more significant in the future.

In closing, I offer my and TLI's assistance in supporting you and the state of MN in our shared vision to secure our cyberinfrastructure, while preserving civil liberties, supporting talent development and economic growth for our state and beyond. My colleagues and I remain at your service to shape together a more resilient, safer and more secure future for our communities, for our state, our nation and the world. Thank You.

On Establishing a Legislative Commission on Cyber Security

S. Massoud Amin, D.Sc.
Director & Honeywell HW Sweatt Chair, Technological Leadership Institute
Professor of Electrical & Computer Engineering
University Distinguished Teaching Professor
University of Minnesota

Chairman, IEEE Smart Grid
Chairman, Board of Directors, Texas Reliability Entity (TRE)
Director, Board of Directors, Midwest Reliability Organization (MRO)

Minnesota Senate
March 9th, 2017

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

What is in the news?

Congressional Research Service Report (CRS) report* this month:

- "The increasing frequency of cyber intrusions on industrial control systems of critical infrastructure is a trend of concern to the electric utility industry,"
- "The National Security Agency reported that it has seen intrusions into [industrial control] systems by entities with the apparent technical capability 'to take down control systems that operate U.S. power grids, water systems and other critical infrastructure,"

Use of a program, called BlackEnergy, to break into systems, steal information and wipe the system completely if/when they are discovered:

- "Hackers are reported to have used the BlackEnergy Trojan horse to deliver plug-in modules used for several purposes, including keylogging, audio recording, and grabbing screenshots. Researchers looking at the BlackEnergy malware are reported to have identified a plug-in that can destroy hard disks, and believe that the attackers will activate the module once they are discovered in order to hide their presence."

Also please see the earlier Office of Personnel Management's system reports.

In summary: The number of attacks on our power grids is astonishing, and the power grids aren't the only thing that are in danger… our entire infrastructure is at risk.

*Cyber: www.fas.org/sgp/crs/misc/R43989.pdf, June 2015
Physical: www.fas.org/sgp/crs/homesec/R43604.pdf, June 2014

Technological Leadership Institute | University of Minnesota Driven to Discover℠

Technological Leadership Institute | University of Minnesota Driven to Discover℠

Currently, there are 16 industry sectors defined as critical infrastructure

85% of critical infrastructure is in private sector *hands*[1]

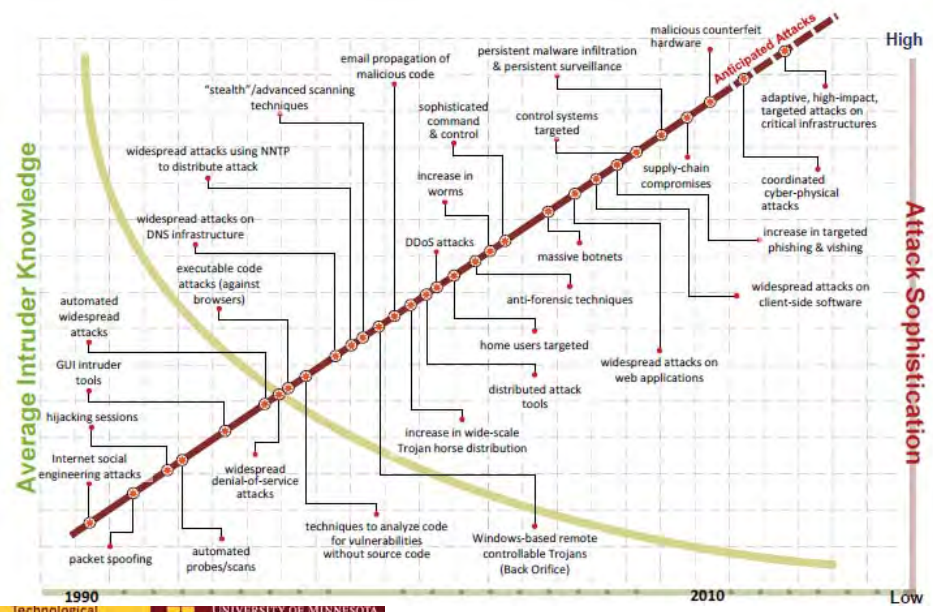
Trends exposing industry to increased risk
- Interconnectedness of sectors
- Proliferation of exposure points
- Concentration of assets

- Agriculture and Food
- Banking and Financial Services
- Chemical
- Commercial Facilities
- Communications
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems
- Critical Manufacturing

1 GAO Report, Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. July 2007, http://www.gao.gov/assets/100/95010.pdf

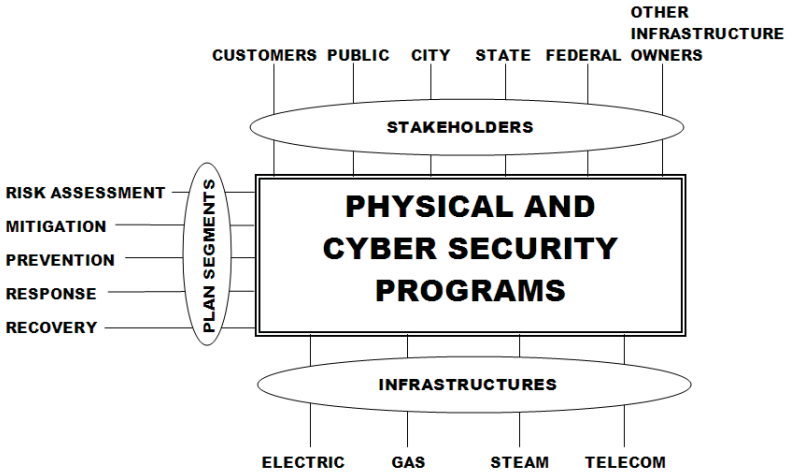
Technological Leadership Institute | University of Minnesota Driven to Discover℠

Cyberattacks – Power Grid Intruder Knowledge



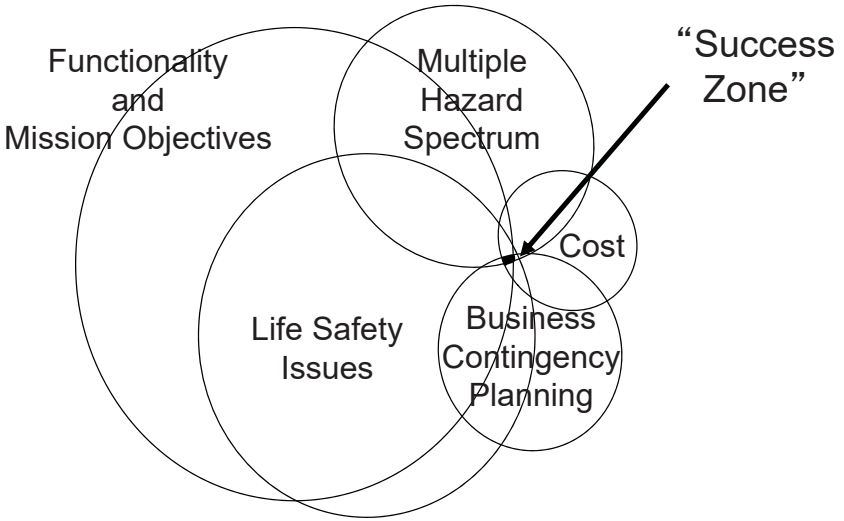
Technological Leadership Institute | University of Minnesota Driven to Discover℠

My background: CIP programs in the industry, government, and the academy



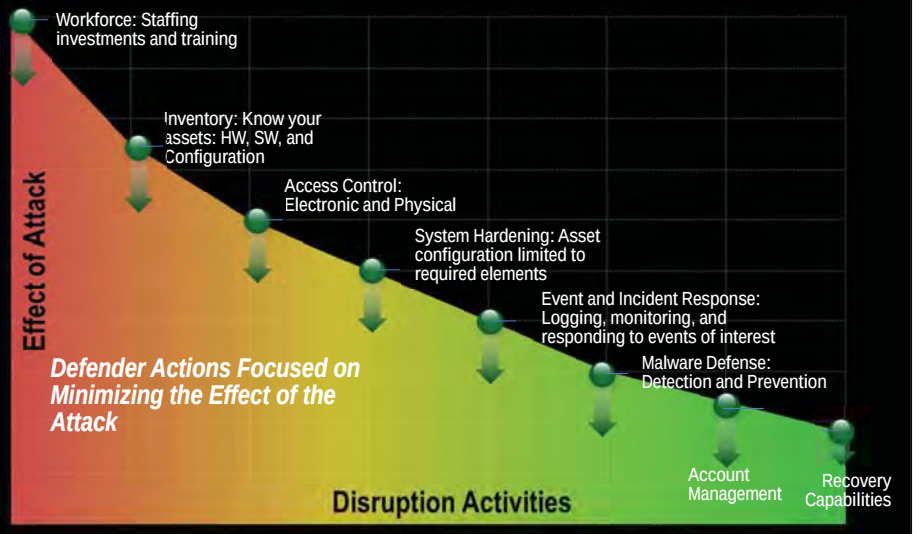
Technological Leadership Institute | University of Minnesota Driven to Discover℠

Real world solutions may be elusive



Technological Leadership Institute | University of Minnesota Driven to Discover℠

Take Action!



Mitigations

Security: What issues impede Protection

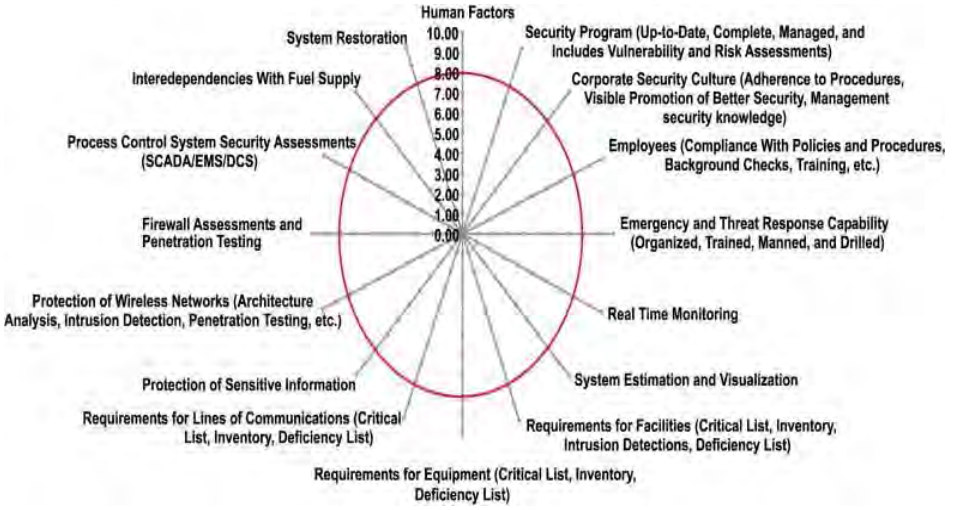
- Inability to share information
- Increased cost of security
- Widely dispersed assets
- Widely dispersed owners and operators
- Finding training and empowering security personnel
- Commercial off-the-shelf (COTS) controls and communications
- Siting constraints
- Long lead-time equipment
- Availability of restoration funds
- R&D focused on vulnerabilities

Prioritization: Security Index

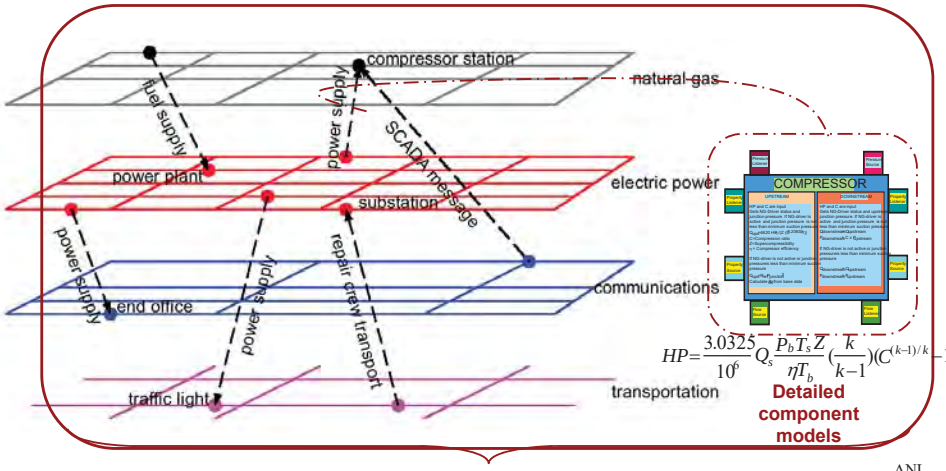
General	Corporate culture
	Security Program
	Employees
	Emergency and threat response capability
Physical	Requirements for facilities, equipment and lines of communication
	Protection of sensitive information
Cyber and IT	Protection of wired and wireless networks
	Firewall assessments
	Process control system security assessments

Assessment & Prioritization:

A Composite Spider Diagram to Display Security Indices



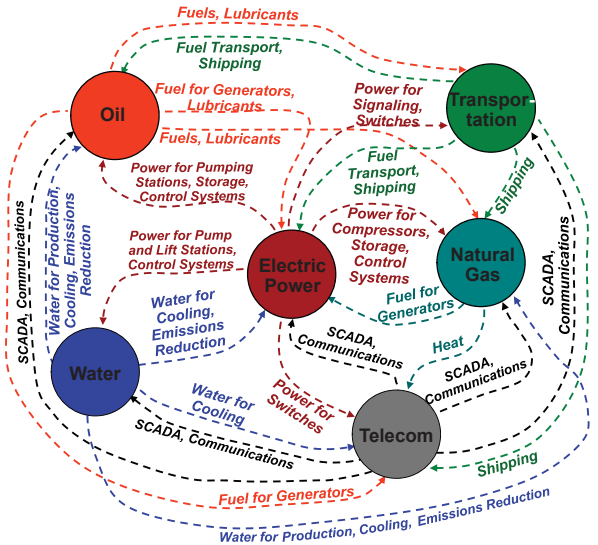
Infrastructure Interdependencies



ANL

- *Critical system components*
- *Interdependence propagation pathways and degree of coupling; Benefits of mitigation options*

Infrastructure interdependency is upon us



ANL -- Peerenboom, Fisher, and Whitfield, 2001

Types of Interdependencies

- Physical (e.g., material output of one infrastructure used by another)
- Cyber (e.g., electronic, informational linkages)
- Geographic (e.g., common corridor)
- Other (e.g., dependency through financial markets)

Smart Grids: What are we working on at the University of Minnesota?

- Integration and optimization of storage devices and PHEVs with the electric power grid
- Grid agents as distributed computer
- Fast power grid simulation and risk assessment
- Security of cyber-physical infrastructure: A Resilient Real-Time System for a Secure & Reconfigurable Grid
- Security Analyses of Autonomous Microgrids: Analysis, Modeling, and Simulation of Failure Scenarios, and Development of Attack-Resistant Architectures

University of Minnesota Center for Smart Grid Technologies (2003-present)
Faculty: Professors Massoud Amin and Bruce Wollenberg
PhD Candidates/RA and Postdocs: Anthony Giacomoni (PhD'11), Jesse Gantz (MS'12), Laurie Miller (PhD'13), Vamsi Parachuri (part-time PhD candidate, full-time at Siemens), Sara Mullen (Phd'09)
PI: Massoud Amin, Support from EPRI, NSF, ORNL, Honeywell and SNL

Overview

- Microgrids
  - U of M - Morris campus project
  - UMore Park Project
  - Controller architecture
  - Resiliency
  - Dollars and watts -- Prices to devices
  - Storage and Renewables integration
  - Autonomous Microgrids
  - Big Data
- Smart Grid U™
- MN Smart Grid Coalition (2008-11) /Governor's Summit '14
- IEEE Smart Grid
- FERC, NERC, Texas RE, and MRO

Technological Leadership Institute | University of Minnesota Driven to Discover℠

I-35W bridge

Just after 6:00 p.m. on Aug. 1, Prof. Massoud Amin was at work in his office on the University of Minnesota's West Bank, where he heard and watched the unthinkable happen—the collapse of the I-35W bridge about 100 yards away.

"As an individual, it was shocking and very painful to witness it from our offices here in Minneapolis," says Amin, director of the Center for the Development of Technological Leadership (CDTL) and the H.W. Sweatt Chair in Technological Leadership. Amin also viewed the tragedy from a broader perspective as a result of his ongoing work to advance the security and health of the nation's infrastructure.

In the days and weeks that followed, he responded to media inquiries from the BBC, Reuthers, and the CBC, keeping his comments focused on the critical nature of the infrastructure. He referred reporters with questions about bridge design, conditions, and inspections to several professional colleagues, including Professors Roberto Ballarini, Ted Galambos, Vaughan Voller, and John Gulliver in the Department of Civil Engineering and the National Academy of Engineering Board on Infrastructure and Constructed Environment.

For Amin, Voller, and many others, the bridge collapse puts into focus the importance of two key issues—the tremendous value of infrastructure and infrastructure systems that help make possible indispensable activities such as transportation, waste disposal, water, telecommunications, and electricity and power, among many others, and the search for positive and innovative ways to strengthen the infrastructure.

Technological Leadership Institute | University of Minnesota Driven to Discover℠

To improve the future and avoid a repetition of the past:

Sensors built in to the I-35W bridge at less than 0.5% total cost by TLI alumni


Terry Ward


Heidi Hamilton


Val Svensson


Joe Nietfeld

Technological Leadership Institute | University of Minnesota Driven to Discover℠

Not Just Utilities … Our Role in Minnesota:
2015 MN2050 Survey

MN 2050 Infrastructure planning, long term success

	2015 Values				
	Small City	Large City	County	State	Total
Roads	$4,174,022,424	$10,517,476,430	$27,647,815,260	$29,338,312,840	$71,677,626,954
Bridges	$1,151,894,172	$807,350,570	$1,456,009,206	$6,592,940,562	$10,008,194,510
Transit	$0	$0	$0	$0	$0
Traffic	$14,168,440	$138,820,460	$59,985,398	$0	$212,974,298
Buildings	$7,583,657,510	$13,724,959,690	$4,869,723,674	$501,696,056	$26,680,036,930
Water	$1,499,020,952	$6,279,799,230	$0	$0	$7,778,820,182
Waste Water	$1,704,463,332	$4,244,983,540	$0	$6,494,782,638	$12,444,229,510
Storm sewer	$0	$2,085,960,070	$0	$0	$2,085,960,070
Storm ponds	$150,185,464	$65,757,060	$5,453,218	$0	$221,395,742
Airports	$1,240,446,922	$1,344,366,560	$0	$0	$2,584,813,482
Ports	$0	$0	$0	$0	$0
Rail	$0	$0	$3,173,772,876	$0	$3,173,772,876
Electrical	$0	$10,564,967,640	$0	$0	$10,564,967,640
Solid Waste	$0	$94,982,420	$796,169,828	$0	$891,152,248
Natural Gas	$2,056,549,066	$2,747,183,840	$0	$0	$4,803,732,906
Total	**$19.5B**	**$52.6B**	**$38.0B**	**$42.9B**	**$153B**

Critical Features of Survivable Systems: Lessons from September 11

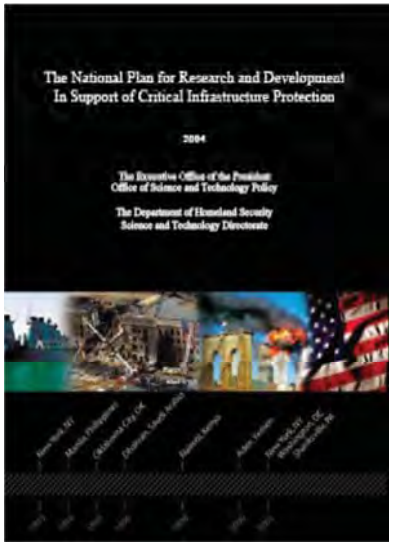
- ⌘ resilience: ability to recover quickly
- ⌘ robustness: failure-resistant through design and/or construction
- ⌘ redundancy: duplicative capacity for service delivery

Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Natural Hazards Research and Applications Information Center, University of Colorado, Boulder, 2003

THE NATIONAL PLAN FOR RESEARCH AND DEVELOPMENT IN SUPPORT OF CIP

- **The area of self-healing infrastructure has been recommended by the White House Office of Science and Technology Policy (OSTP) and the U.S. Department of Homeland Security (DHS) as one of three thrust areas for the National Plan for research and development in support of Critical Infrastructure Protection (CIP).**



Providing reliable and resilient systems requires organizations that can

- ⌘ Anticipate
- ⌘ Plan
- ⌘ Implement
- ⌘ Adapt and improvise

MN and Regional Partnerships: Means to Identify/Validate Needs/Foster Preparedness

- **Major benefits from encouraging and supporting creation of MN and regional cyber security partnerships**
  - Help identify Cyber CIP requirements
  - Expedite cross-sector and cross jurisdiction coord. and collaborative implementation of solutions
  - Assist in mission assurance
  - Facilitate information sharing on threats and disruptions
  - Facilitate coordination among regions, thereby fostering interoperability
  - Serve as test-beds for pilot projects
  - Support and assist smaller local entities

Looking Beyond Interdependencies: Other Pressing Infrastructure Security Issues

Current focus on technical, practitioner-related challenges—Tyranny of the In-Box

Not Being Adequately Addressed:

- Building the necessary policy foundation that addresses legal, ethical, and defense in depth issues in assuring Local/State/National/Global infrastructures
- Long-term analysis of what technology, political and economic developments will have far-reaching repercussions for securing infrastructures and keeping them secure (with Economic Growth opportunities)

Technological Leadership Institute | University of Minnesota Driven to Discover℠

Discussion Questions

- What level of threat is the industry responsible for, and what does government need to address?
- Will market-based priorities support a strategically secure power system?
- What system architecture is most conducive to maintaining security?

Technological Leadership Institute | University of Minnesota Driven to Discover℠

BASIS OF FUTURE COMPETITION

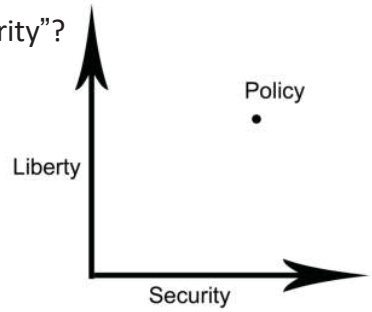
The speed at which an Enterprise can

- Gather
- Collate
- Analyze
- Apply information

Can we build non-intrusive yet high confidence tools, systems, processes that increase our security AND preserve/extend our civil rights?

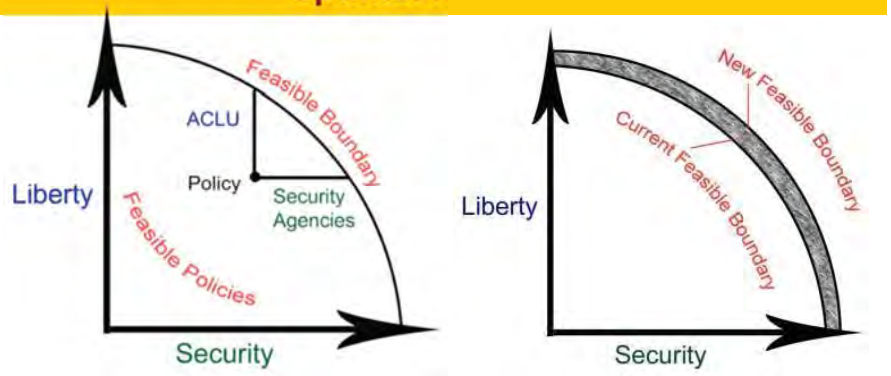
Synergy Between Security Technologies & Policy

- Incorporate security and privacy early as "design criteria"
- Provide policy impact statement
  - E.g. tradeoffs between "liberty & security"?
  - Non/low-intrusive but high confidence technologies analogous to "MRI"
  - Plot the space



Technological Leadership Institute | University of Minnesota Driven to Discover℠

Where is a given policy w.r.t. -a theoretically optimal frontier?

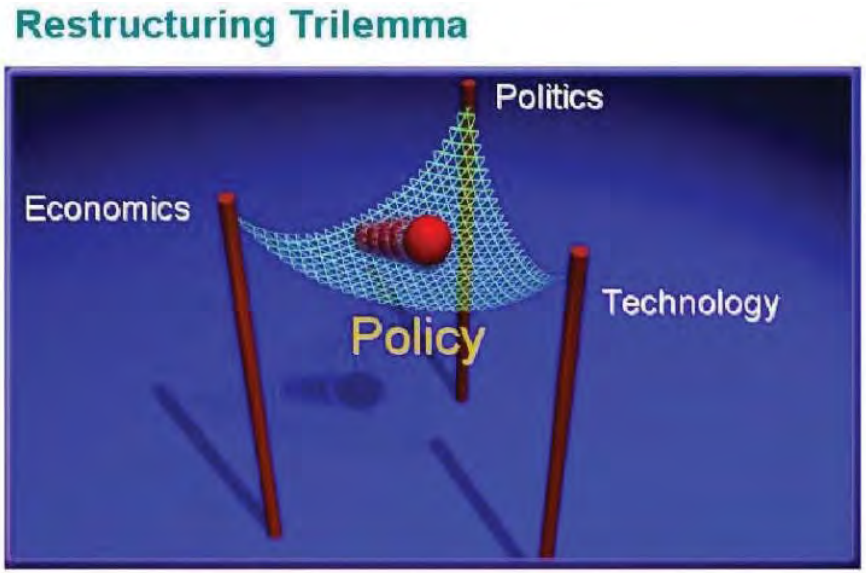


Implications for new technologies -some offer more "L" or more "S"

-What if we offer both?
-Can this be a design criteria?

E.g. remote monitoring; anomaly detection; wide-area tamper detection

Unresolved Issues Cloud Planning for the Future



Observations and the Road Ahead:

- What are the key security, energy, environmental and economic issues facing our cities, our nations, and the world?
- "What are the range of new services enabled by smart grids?"
- Smart grids (enabling Smart Cities, Smart Homes and Buildings) included in all energy legislation
- Potential as an "enabler in state and federal regulatory policies" to drive economic growth

Technological Leadership Institute

TECHNOLOGICAL LEADERSHIP INSTITUTE

ABOUT US

TLI was established in 1987 by an endowment from the Honeywell Foundation.

Est.1987
Honeywell

The Institute is one of 12 academic centers affiliated with the **College of Science and Engineering**, which is ranked among the top engineering and science degree programs in the country.

OUR MISSION

TLI's mission is to develop **local and global leaders** for technology-intensive enterprises through its three Master of Science degree programs.

CONTINUING EDUCATION

TLI partners with local and global organizations to provide applied learning experiences through our professional development and continuing education opportunities.

Technically Speaking: This seminar series features experts and thinkers in business, science and technology.

Rochester signature series: An annual, four-day professional development opportunity focused on local business topics.

Custom short courses: Our customizable short courses provide training tailored to your business or employee needs.

INNOVATIVE LEADER

Dr. Massoud Amin

- Director of TLI
- Father of Smart Grid
- IEEE & ASME Fellow
- University Distinguished Teaching Professor Award Recipient
- Authored 200+ Publications

GRADUATE MINORS

- Management of Technology Minor
- Cyber Security Minor
- Security Technologies Minor

TLI BY THE NUMBERS

Cohort Model with 30 Students

1200+ Alumni

60+ Faculty

10+ Advisory Board Members

EXECUTIVE EDUCATION FOR TECHNOLOGY LEADERS

MOT - M.S. in Management of Technology (MOT)
21-month program aimed at transforming engineering, science and other technical professionals into business leaders.

MSST - M.S. in Security Technologies (MSST)
14-month program designed to shape tomorrow's risk management policymakers and innovators.

MDI - M.S. in Medical Device Innovation (MDI)
14-month program designed to prepare students to manage complex innovation challenges in the global medical technology industry. (*see more on back)

TECHNOLOGICAL LEADERSHIP INSTITUTE

MASTER OF SCIENCE
Management of Technology

The Technological Leadership Institute **Master of Science in Management of Technology (MOT)** degree program is aimed at transforming engineering, science and other technical professionals into business leaders.

Complete Degree in 21 Months

- Work Full Time
- Class Meets 1 Day/Week
- Blends Business & Technology

- 100% — Program Completion Since 2007
- 34% — TLI Grads are Executives in 5 Years

GLOBAL LEARNING

For 21 years the MOT graduate program has sent students all over the world, including **Austria**, **India**, **Czech Republic**, **China**, **Malaysia**, **Singapore**, **Ireland**, **Germany**, **Iceland**, **Taiwan** and **South Korea**.

PROGRAM REQUIREMENTS

- **Undergraduate Degree from Accredited University**
- **Minimum of 5 Years Full-Time Work Experience** in a Tech-Intensive Area
- **Demonstrated Leadership Potential**

Recommended: GPA of 3.0 or Higher
Corporate Endorsement

TECHNOLOGICAL LEADERSHIP INSTITUTE

MASTER OF SCIENCE
Medical Device Innovation

The Technological Leadership Institute **Master of Science in Medical Device Innovation (MDI)** degree program provides early and mid-career medical device professionals the skills needed to be effective leaders.

Complete Degree in 14 Months

- Work Full Time
- Class Meets 2 Days/Week
- 250K — Medical Device Professionals in MN

- 50% — World's Medical Device Companies in MN
- 27% — BLS Expected Job Growth by 2018

OPPORTUNITY

MDI students and graduates are leading the medical device industry and are employed by a variety of companies including:

Boston Scientific · Medtronic · St. Jude Medical · American Medical Systems · Phillips Medisize · Minnesota Eye Consultants, P.A.

PROGRAM REQUIREMENTS

- **Undergraduate Degree** GPA of 3.0 or higher
- **Demonstrated Leadership Potential**
- **Relevant Work Experience**

TECHNOLOGICAL LEADERSHIP INSTITUTE

MASTER OF SCIENCE
Security Technologies

The Technological Leadership Institute **Master of Science in Security Technologies (MSST)** prepares the next generation of security leaders and provides students with the necessary skills to move forward professionally.

Complete Degree in 14 months

- Work Full Time
- Class Meets 2 Days/Week
- 1st — MSST Degree Program in Midwest

- 120% — Growth in Cyber Security Careers
- 20K — Open Information Security Jobs

OPPORTUNITY

MSST students and graduates are leading the growing security technologies industry and are employed by a variety of companies:

Wells Fargo · Best Buy · IBM · Lockheed Martin · Target

PROGRAM REQUIREMENTS

- **Undergraduate Degree** GPA of 3.0 or higher
- **Demonstrated Leadership Potential**
- **Relevant Work Experience**

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
290 McNamara Alumni Center | 200 Oak Street SE
Minneapolis, MN 55455 | Phone: 612.624.1846
Email: tli@umn.edu | tli.umn.edu

Exhibit A

Commission on Enhancing National Cybersecurity

Established by Executive Order 13718, Commission on Enhancing National Cybersecurity

Meeting Agenda

August 23, 2016

University of Minnesota
TCF Bank Stadium
Dairy Queen Room
420 23rd Avenue SE, Minneapolis, MN 55455

*Please note: Speakers/times are subject to change without notice.

Tuesday, August 23, 2016			
9:00 A.M.	–	9:15 A.M.	*Welcome and Overview* o Dr. Massoud Amin, Director, Chair, Technological Leadership Institute; Distinguished University Professor, University of Minnesota
9:15 A.M.	–	11:00 A.M.	*Panel 1: Consumers and the Digital Economy* o Susan Grant, Director, Consumer Protection and Privacy, Consumer Federation of America o Mike Johnson, Director of Graduate Studies in Security Technologies, Technological Leadership Institute, University of Minnesota o Kevin Moriarty, Senior Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (FTC) o Sarah Zatko, Chief Scientist, Cyber Independent Testing Laboratory (CITL)
11:00 A.M.	–	11:15 A.M.	*Break*
11:15 A.M.	–	1:00 P.M.	*Panel 2: Innovation (Internet of Things, Healthcare, and Other Areas)* o Robert Booker, Senior VP, Chief ISO, UnitedHealth Group, Optum, Inc. o Brian McCarson, CTO, Intel IoT Strategy; Sr. Principal Engineer, Chief Architect, Intel IoT Platform o Gary Toretti, Chief ISO, Sabre Corporation
1:00 P.M.	–	2:00 P.M.	*Lunch*
2:00 P.M.	–	3:45 P.M.	*Panel 3: Assured Products and Trustworthy Technologies* o Edna Conway, CSO, Global Value Chain, Cisco Systems, Inc. o Joshua Corman, Director, Cyber Statecraft Initiative; Former CTO, Sonatype; Co-Founder, I am The Cavalry and Rugged Software o Ken Modeste, Global Cybersecurity Technical and Strategy Lead, Underwriters Laboratories Inc. (UL) o Dr. Ron Ross, Computer Scientist, National Institute of Standards and Technology (NIST)
3:45 P.M.	–	4:00 P.M.	*Public Comment*
4:00 P.M.	–	5:00 P.M.	*Commission Discussion*
5:00 P.M			*Meeting Adjourned*

Open Meeting of the Presidential Commission on Enhancing National Cybersecurity
Hosted by the Technological Leadership Institute, University of Minnesota
Invitation: http://tli.umn.edu/Commission-on-Enhancing-National-Cybersecurity.
Remarks by Dr. S. Massoud Amin
August 23, 2016

Mr. Chairman, Distinguished Commissioners, panelists, NIST staff, Colleagues and guests. Good morning. I am Massoud Amin, and on behalf of the University of Minnesota Technological Leadership Institute, more commonly referenced as TLI, we welcome you. We are honored to host this timely meeting and thank you for your leadership in helping ensure the security of our nation.

The University of Minnesota has had a long, distinguished history of pioneering contributions to security. I have had the distinct honor to be a part of it as a professor of electrical & computer engineering where I continue my R&D projects toward secure self-healing smart grids and as director of the Technological Leadership Institute. For nearly three decades, TLI has been developing the next generation of technological leaders through our Master of Science degrees, and since 2009 in the Master of Science Security Technologies degree program. Our more than 1300 alumni of our graduate programs are successfully innovating in all areas of technology in more than 400 enterprises - and nearly 180 of them are focused on security – including the areas in today's dialogue, which we cover in the Security Technologies degree program here at the University.

You will hear from experts who will provide a summary of the State of our cyber security– Activities, Accomplishments, Opportunities and Challenges ahead. We will also review the evolving spectrum of cybersecurity threats and countermeasures, which continue to improve yet poses novel threats, in several areas including:

- Challenges confronting consumers in the digital economy
- Innovation (Internet of Things, healthcare, and other critical infrastructure areas)
- Assured products and services.

The more recent spectra of vulnerabilities (privacy concerns in an increasingly interdependent digital world, cyber-attacks and sophisticated malware, to personal privacy, safety and security) have been in the spotlight while our national and international critical infrastructures face new challenges.

Critical infrastructures such as energy, power and electric power grid, banking and finance, oil/gas/water pipelines, transportation, food/agriculture, health services, manufacturing, public health, financial systems, and telecommunications information networks including the Internet and embedded digital systems have become increasingly important, interdependent, critical and complex.

The security challenges of protecting human safety and the critical infrastructure in the United States and throughout the World have been highlighted during the last few decades. Worldwide cyber-attacks are on the rise with evolving spectra of threats and more sophisticated adversaries:

First, cyber-related RISK is significant:
The threat is real - The Vulnerabilities are widespread - And the Consequences can be disastrous

Cybersecurity threats represent one of the most serious national security, public safety and economic challenges we face as a nation. Understanding the dynamically evolving threats and emerging risk and our ability to assess and manage quickly changing risks is more important now than ever before.

President Obama's executive order, of February 12, 2013, highlights the cyber threat is one of the most serious economic and national security challenges we face as a nation and that America's economic prosperity in the 21st century will depend on cybersecurity. It provides a "framework" to effectively allow intelligence to be gathered on cyberattacks and cyber threats to privately owned critical national infrastructure — such as the private defense sector, utility networks, and the banking industry — so they can better protect themselves.

The very technologies that empower us to lead and create also empower those who would disrupt and destroy… our public and private enterprises, including corporate and government networks are constantly probed by intruders.

Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

Second, the challenges abound:

- Telecommunications and information processing (our) systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation,
- And technologies to exploit these electronic systems is widespread and is used extensively.

BOTTOM LINE: The RISK is significant and the issues numerous and growing.

The answer to these challenges will undoubtedly take extended our discussions today.

In addition, since I was asked by the Commission to provide my input on addressing Digital Security and recommendations for action, enclosed please find an addendum outlining my detailed thoughts and recommendations provided for your reference on the next few pages. These are a subset recommendations, which I drafted in partnership and on behalf of the IEEE to advise the U.S. President's Quadrennial Energy Review (QER). Our team completed a report that provides guidance on grid-related developments to the U.S. Department of Energy and the White House for the nation's first-ever Quadrennial Energy Review.

As noted therein, the cost of developing and deploying a modernized, stronger, more secure and smarter critical infrastructure for the country is cost effective and should be thought of as an investment in the future.

In closing, I thank you for bringing this important dialogue to the University of Minnesota. We welcome our continued collaborations and look forward to maintaining our place together at the forefront of proactively addressing and confronting these security challenges.

*** * * * Thank you * * * ***

Addendum:

Question 1: *What do you feel is the most important thing the electric regulatory industry should accomplish over the next five years?*

Answer: It is imperative that we reduce uncertainty for investments in the grid, in innovation and research and development, in modernizing entire systems and encouraging development of capable human capital. Think systems, be forward thinking, be strategic, know the past, be open to innovation, develop a fresh outlook at what can realistically be achieved—what are the resultant primary, secondary and tertiary consequences? I quote HL Mencken, "For every complex problem, there's a single solution that is simple, neat and wrong!" Develop capabilities to understand and address such interdependent complex systems. As these systems interact with each other, there are many solutions that can come together under what we call design thinking. It involves care, patience, time and resoluteness not to fail. For more information on these thoughts, please read my article, "We are not in Kansas anymore" in the September/October 2011 edition of the Midwest Reliability Organization (MRO) newsletter.

Question 2: What are the persisting security concerns and why can be done?

Answer: As CIP 5 and cyber-physical programs are implemented and protections put into place, difficult choices will have to be made about how to handle a number of trade-offs:

- **Outdated regulatory framework.** One important constraint on regulatory oversight of security protection is the split jurisdiction over the grid, which is keeping us locked into the 20th century infrastructure. The bulk electric system is under federal regulation but the distribution grid, metering, and other aspects of the grid are regulated by individual states. Overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships, thus a new model for these relationships is required for infrastructure security. For instance, a stockpiling authority, be it private or governmental, could obtain long lead-time equipment based on the power industry's inventory of critical equipment, which must include the number and location of available spares and the level of interchangeability between sites and companies. Clearly, further standardization of equipment will reduce lead times and increase the interchangeability of critical equipment. For example, the typical, state-level regulatory approach – cost-of-service rate making and volumetric pricing – puts IOUs and microgrids at odds. Most states regulate synchronous interconnections based on IEEE 1547 (please see section 1 of the IEEE QER report for more details) and FERC's small generator interconnection procedures (SGIP) in FERC Order 2006.

- **Controls and Communication** - Protection of power generation, transmission and distribution equipment is insufficient to guarantee delivery of electricity because widespread, coordinated denial of control and communication systems could cause significant disruption to the power grid. This includes SCADA systems, communications between control systems, monitoring systems and business networks. However, the power management control rooms are currently well-protected physically, although they may have cyber vulnerabilities. NERC

requires a backup system and there are also manual workarounds in place. The Federal Energy Regulatory Commission (FERC) is working toward a common set of security requirements that will bring all electric sector entities up to at least a minimum level of protection.

- **Investments in security**. Although hardening some key components—such as power plants and critical substations—is highly desirable, providing comprehensive physical protection for all components is simply not feasible or economical. Dynamic, probabilistic risk assessments have provided strategic guidance on allocating security resources to greatest advantage. However, pathways to cost recovery and making a business case for security investments/upgrades, often pose challenges.

- **Security versus efficiency and ROI.** The specter of future sophisticated terrorist attacks raises a profound dilemma for the electric power industry, which must make the electricity infrastructure more secure, while being careful not to compromise productivity. Resolving this dilemma will require both short-term and long-term technology development and deployment along with supportive public policy for cost recovery, which will affect fundamental power system characteristics, spurring development of new business models/strategies.

- **Centralization versus decentralization of control.** For several years, there has been a trend toward centralizing control of electric power systems. The emergence of regional transmission organizations, for example, promised to greatly increase efficiency and improve customer service. But we also know that terrorists can exploit the weaknesses of centralized control; therefore, smaller and local semi-autonomous systems would seem to be the system configuration of choice (analogous to platoons during warfare with local autonomy, while coordinated with the overall mission of the operation). In fact, strength and resilience in the face of attack will increasingly require the ability to bridge simultaneous top-down and bottom-up decision-making in real time—fast-acting and totally distributed at the local level, coordinated at the mid-level and aligned with executive objectives.

What are some specific examples and actions required to improve security and resilience of the system?

✓ ***POLICY REMAINS THE SINGLE BIGGEST INFLUENCE ON THE BUSINESS CASE***

Example -- Microgrids: A 2013 white paper, "Results-based Regulation: A Modern Approach to Modernize the Grid," addresses the limitations of cost-of-service regulation and offers alternative regulatory models that each state could consider adopting.

A recent study of policies relating to microgrid adoption in Minnesota reveals that state regulatory policies often don't address microgrids at all. But the Minnesota study suggests that state policy define and acknowledge the opportunities presented by microgrids to achieve state policies regarding

energy surety and the adoption of renewable energy sources and to "ensure that microgrids are properly valued and considered in energy resource and policy initiatives." The Minnesota study identified both regulatory and legislative steps to achieve these objectives. FERC policy covers DG-related projects up to 20 megawatts (MW) and how they interconnect with interstate transmission systems, relevant if the project plans to sell wholesale power into an independent system operator (ISO). FERC has issued a NOPR that it will amend its SGIP and SGIA (small generator interconnection agreement) to "ensure the time and cost to process small generator interconnection requirements will be just and reasonable and not unduly discriminatory".

State-level PUCs wield the most influence. Many states are reviewing related policies as they balance utility interests with ESCO competition and the needs of the commercial/industrial and residential utility customer sectors. A state-level, results-oriented regulatory approach that rewards utilities for adopting innovations that directly benefit their customers may encourage microgrid adoption.

In terms of a federal role in microgrid-related policy development, states will continue to exercise (and defend) their role in microgrid-related policy-making. With access to resources – possibly facilitated by the U.S. DOE – on related technology and standards, regulatory reform and stakeholder impacts, however, state regulators can create policies that favor microgrid development and balance the diverse interests involved.

FERC's small generator interconnection procedures (devised by SGIP, embodied in FERC Order 2006) also are relevant to this discussion.

State policies may also need to evolve with standards through a regular, consistent process, both to encourage microgrid development and reward utilities for cooperating with a customer benefit that cuts into its revenue. Policy and standards should work in hand-in-hand.

One area ripe for revision: Where a state has a restrictive definition for DG capacity for its interconnection requirements. Current rules require large microgrid proposals to forge unique agreements with a utility at great cost and uncertainty.

California regulators have articulated many of the issues that policy must address, as has the National Regulatory Research Institute. [20] Both efforts provide an in-depth look at the complexity and interrelated nature of many microgrid-related policy issues as utilities, independent system operators, ESCOs, customers and other stakeholders are linked technologically and in wholesale and retail markets.

Critical regulatory issues currently being reviewed include, among many others:

- How costs and benefits are apportioned to myriad stakeholders (and how that affects cost recovery for utilities),
- Whether a microgrid relies on the distribution system (or transmission system) for backup and how that might affect reliability,
- Whether and how to treat non-utility microgrid sponsors as utilities, and
- Multiple possible business models for utilities offering microgrids.

Metrics, Best Practices, and Roadmaps: Establish metrics on workforce and identify policies that facilitate necessary workforce development activities by the regulated companies. There is a workforce crisis coming that could affect customer services and costs so it is in the public interest that regulators increase their oversight of workforce development.

Select a lead organization (perhaps DOE) to facilitate regulator / industry dialog by designing and holding workforce workshops for NARUC, FERC and NERC that create situational awareness for state and national regulators. The NERC System Operator Certification and Training program should be used as an example of a successful program for regulated training. Initially the focus should be on the workforce whose performance is most directly connected to reliability, such as system operators, linemen, planning engineers, protection engineers/technicians and substation operators. DOE can convene a cross functional group of experts to include industry, government agencies (DOL, DOE, NSF, DHS, and DOD) and regulators for the purpose of reviewing current practices in workforce benchmarking and create metrics to quantify the threat posed to the electric grid's performance by insufficient replacement workers. DOE could seek out opportunities to co-fund industry education and training programs (IEEE examples include Scholarship Plus, WISE, Plain Talk) and fund student and innovation competitions.

Improving Existing Survey and Assessment Tools: In generation, FERC has in the Form-1 a large amount of the material needed to support an assessment of the adequacy of the generation fleet. There are operational and maintenance aspects that are not included in the Form-1. FERC Forms 714 and 715 provide some, but not all of this information and Form 556 provides information on smaller generation facilities. Again the existing FERC data would not provide a complete survey, but it is a strong starting point to develop survey results from. For sales, forecasts, usage, and other consumption related information the Energy Information Agency (EIA) provides the best starting point.

Recommendation for a survey of the electrical infrastructure:

- Bring together the industry and end-user stakeholders to look at the existing survey tools, and define the overall needs for an industry wide set of survey tools. This working group should provide a clear requirements document on what needs to be surveyed, and the depth that the survey needs to cover.
- Determine what existing materials can be used to support the survey requirements, minimizing new data collection.
- Provide adequate resources to complete a survey tool set that supports the requirements that were developed by the stakeholder group and uses the data from existing sources.
- Working with an industry working group, define how the survey tool will be used both improving the infrastructure and in any regulatory actions. The tool set will fail, if there is no consensus among the stakeholder groups. A solid survey tool set for both self-assessments will provide a data driven way for the industry to determine where to focus research, standards development, training, staffing, and operational improvements for the industry. With the rapid changes in the environment this will allow the better deployment of scare resources.

Pertinent IEEE QER recommendations to the U.S. DOE, for your consideration:

Markets and Policy

- Use the National Institute of Standards and Technology (NIST) Smart Grid Collaboration or the NARUC Smart Grid Collaborative as models to **bridge the jurisdictional gap** between the federal and the state regulatory organizations on issues such as technology upgrades and system security.
- More transparent, participatory and **collaborative discussion** among federal and state agencies, transmission and distribution asset owners, regional transmission operators (RTOs) and independent system operators (ISOs) and their members and supporting research is needed to improve these parties' understanding of mutual impacts, interactions and benefits that may be gained from these efforts.
- Continue working at a federal level on better **coordination of electricity and gas markets** to mitigate potential new reliability issues due to increasing reliance on gas generation; and update the wholesale market design to reflect the speed at which a generator can increase or decrease the amount of generation needed to complement variable resources.

Asset Management:

- Support **holistic, integrated approach** in simultaneously managing fleet of assets to best achieve optimal cost-effective solutions addressing the following: **Aging infrastructure, Grid hardening (including weather-related events, physical vulnerability, and cyber security) and System reliability**.
- **Urgently address managing new Smart Grid assets** such as advanced metering infrastructure (AMI) and intelligent electronic devices.
- Encourage utilities to investigate practical measures to shorten times to replace and commission equipment failures due to extreme events or other reasons.
- In the case of long-duration interruptions, all utilities should adopt improved measures to provide customers with a timely estimate of when power is to be restored.
- When extreme events occur it is important for post-event reviews to determine impacts and lessons learned for better management of future events.
- Infrastructure security requires a **new model for private sector-government relationships**. Overlapping and inconsistent roles and authorities hinder development of productive working relationships and operational measures.
- Perform **critical spares and gap analysis**. A detailed inventory is needed of critical equipment, the number and location of available spares and the level of interchangeability between sites and companies. Mechanisms need to be developed for stockpiling long lead-time equipment and for reimbursement to the stockpiling authority, be it private or government. Other approaches include standardizing equipment to reduce lead times and increase interchangeability.
    - U.S. DOE should continue to work with industry to ensure that the protection of spares and all assets is carried out and that transportation of large equipment is feasible. We

further recommend actions that might lure domestic manufacturing back into the U.S. for units 300 KV and above. (Progress in this area has been made with post-9/11 efforts initiated by EPRI's Infrastructure Initiative in September 2001 to March 2003, as well as with the EEI STEP (Spare Transformer and Equipment Program), which has been in place since 2004. Utilities should also continue to work with industry and manufacturers to expand the existing self-healing transformer programs, such as efforts now underway by EPRI and ABB. Further, many utilities have mutual aid agreements on spares.

- Increased federal R&D for emerging technologies that may impact T&D grids, including new types of generation, new uses of electricity and energy storage, with an additional focus on deployment and integration of such technologies to improve the reliability, efficiency and management of the grids.
- Application of proactive widespread condition monitoring, integrating condition and operational data, has been shown to provide a benefit to real-time system operations, both in terms of asset use and cost-effective, planned replacement of assets.

Reliability, Security, Privacy, and Resilience

- Facilitate, encourage, or mandate that secure sensing, "defense in depth," fast reconfiguration and self-healing be **built into the infrastructure**.
- Mandate consumer data **privacy and security for AMI systems** to provide protection against personal profiling, real-time remote surveillance, identity theft and home invasions, activity censorship and decisions based on inaccurate data.
- Support alternatives for utilities that wish to reduce or eliminate the use of wireless telecom networks and the public Internet where there might be concerns about increased grid vulnerabilities. These alternatives include the ability for utilities to obtain private spectrum at a reasonable cost.
- Improve **sharing of intelligence and threat information** and analysis to develop proactive protection strategies, including development of coordinated hierarchical threat coordination centers – at local, regional and national levels. This may require either more security clearances issued to electric sector individuals or treatment of some intelligence and threat information and analysis as sensitive business information, rather than as classified information. National Electric Sector Cybersecurity Organization Resource (NESCOR) clearing house for grid vulnerabilities is an example of intelligence sharing.
- Speed up the development and enforcement of **cyber security standards**, compliance requirements and their adoption. Facilitate and encourage design of security from the start and include it in standards.
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).