NIST Response – Cybersecurity Education at the Technological Leadership Institute (tli.umn.edu) at the University of Minnesota

General Information

Are you involved in cybersecurity workforce education or training (*e.g.,* curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?

The Technological Leadership Institute's (TLI, tli.umn.edu), Master of Science in Security Technologies (MSST) program at the University of Minnesota is actively involved in creating and delivering cybersecurity education for future security leaders. We offer a full professional master's degree in security technologies with a focus on cyber security and its connection to critical infrastructure protection.

What are we doing at the U of M? Minnesota has had a long distinguished history of pioneering pivotal contributions to technology. TLI was established in 1987 at the University of Minnesota with an endowment from the Honeywell Foundation with the mission of developing leadership programs for fast-tracked professionals in technology-intensive sectors of the economy.

As an interdisciplinary center, TLI brings together seven distinguished university endowed chairs who are at TLI; 64 world-class faculty members from across 10 colleges and three centers at the University; and 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, as well as research and consulting projects that leverage expertise in industry, government and academia. TLI cuts across departmental and college boundaries to bring together 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 to serve communities in Minnesota and beyond through our education, research and outreach.

Nearly all of TLI's 1,300+ M.S. recipients and 1,250+ alumni of short courses are currently working in more than 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

Management of Technology (MOT) alumni, more than 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 (DHS) initiated a partnership with our Master of Science in Security Technologies (MSST) program for an event on cyber security in Minnesota. TLI works closely with the U.S. DHS and the Naval Postgraduate School on a security curriculum. We welcome the continued collaborations and look forward to maintaining our place together at the forefront of securing 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, the MSST program is well-aligned with state, national and international priorities; it looks beyond "dogs, guns, cameras and guards" toward the increased role of cyber security, science and technology in protecting our critical assets, making our nation safer and more productive, and our economy more secure.

TLI staff and Dr. Amin have had numerous collaborations with NIST (Dr. Ron Ross and other colleagues) during the past 14-15 years. The most recent one was to host the NIST/White House Commission on Enhancing National Cybersecurity (https://tli.umn.edu/Commission-on-Enhancing-National-Cybersecurity). The public meeting was held on Tuesday, August 23, 2016, from 9 a.m. to 5 p.m. at TCF Bank Stadium at the UofM. The Commission, along with expert panelists, addressed the following topics: challenges confronting consumers in the digital economy; innovation (Internet of Things, healthcare, and other areas); and assured products and services. Dr. Massoud Amin, director of the Technological Leadership Institute, gave the opening remarks, and Mike Johnson, director of graduate studies for the M.S. in Security Technologies degree program, was one of the expert panelists selected to address the Commission on the topic of challenges confronting consumers in the digital economy. There were about 240 attendees.

In addition, TLI created and delivers a number of other professional educational offerings, including:

- Rochester Signature Series: annual 4-day short course offering in partnership with May Clinic, IBM and other industry stakeholders (includes modules on cybersecurity)
- Cyber Security Summit: The Cyber Security Summit, http://cybersecuritysummit.org/, which Dr. Massoud Amin created in 2010, as an outreach for our Master of Science for Security Technologies (MSST) program, continues to very successful, locally, nationally and globally; last year attendance was over 700
- MN National Guard – Croatia program: 5 days of course offerings delivered in Croatia as part of MN National Guard partnership with Croatia defense ministry
- Short Courses & Consulting: recently developed a portfolio of non-credit short courses to be offered in corporate settings
- In addition, TLI reaches out to the broader community through targeted seminars and customized training/short courses that reflect the expertise of her faculty and current needs of local organizations. TLI has had over 2400 alumni of our 2-, 4-, 8-, and 12-day programs.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. **What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?**

While there are metrics available on the number of individuals that have successfully completed cybersecurity-related certification programs such as the CISSP, CISM, CEH, and other specific skills certificates, and metrics pertaining to successful graduates of our own TLI MSST program, there are limited aggregated metrics and information on security skill levels of graduating students or self-taught/employer-taught staff. Public media and vendor-sponsored research has provided estimated skills gaps (e.g. 1.5 million open cybersecurity jobs by 2019, etc.), but finding valid data on how we are doing with transferring cybersecurity skills to current or potential employees is lacking.

Having a mechanism to collect the number of annual graduates from two and four-year programs with degrees that fall within a defined cybersecurity skills category would be helpful to gauge both progress in improved cybersecurity education initiatives and potential validation that the training these graduates receive is effective and adequately meets the needs of organizations.

On a regional scale, Minnesota has organizations (example: Minnesota Cyber Careers Consortium, MNC3 - http://mnc3.org/) that are focusing on improving this data gap by promoting initiatives that evaluate the level of cybersecurity education available from K-12 through advanced degrees and by collecting information on employer gaps and perceived needs. More effort is needed to improve the quantity and quality of measurable data related to this issue in order to more effectively measure and manage work efforts and outcomes.

2. **Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?**

While TLI uses the NICE Cybersecurity Workforce Framework (and related components) when providing instruction on security operations organizations and roles, we are challenged with the substantive revisions that have been applied to this framework since its release. There does not appear to be consensus at this time on the categories and skills that are needed in an effective security organization. Outside of this example, there appears to be little awareness of the skills definitions, especially among employers.

There also appears to be a problem with consistency of industry labels for various skills groups, frequently influenced by buzzwords of the day. A consistent framework would assist in better understanding organizational structure expectations in the cybersecurity arena and measuring the adequacy/success of cybersecurity education in meeting the needs of organizations.

3. **Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?**

N/A. TLI is a specialized educational organization within the University of Minnesota, and our workforce does not have a specific role in securing technology systems at the University. We do not have this information as it relates to the broader University security organization.

4. **What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)?**

Organizational needs for cybersecurity skills within their workforce are impacted by the industry/sector, size, IT and security maturity of the organization, although all organizations ultimately need similar skill sets within their organizational tool kit (either internally staffed or through trusted providers). Most organizations tend to default to the very specific needs they perceive due to purchased technologies or regulatory requirements, which results in a large number of employers looking for the same, often very limited resource (automated resume readers looking for keywords of a targeted product or narrow skill, of which there are not very many applicants matching). Because of this often-narrow view of needed resources, employers are often frustrated and regularly report gaps in available skilled employees versus positions needing to be filled. It will likely take a combination of better educated graduates and organizations with more flexibility in training teams to meet their specific needs to address this issue.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

It is our opinion that cybersecurity employees need a combination of specific technical skills and soft skills including business operations and management context in order to be effective. Graduates who have fundamental technology skills and the tools to learn about the dynamic systems that are prevalent in security organizations will be best able to cope with the rapidly changing technology and threat landscape. We also find value from experiences gained by our students after they graduate from their undergraduate program before joining the MSST program. Work experience within an organization of any type provides valuable context for understanding complexity and designing usable security solutions.

6. **What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?**

The greatest challenges facing the Nation are the persisting and evolving spectra of threats and vulnerabilities. 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. In summary:

1. **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. **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. The technology to exploit these electronic systems is widespread and used extensively.

3. **Various groups and committees that have studied 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 program to identify the top five 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 & e-commerce
- 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
- Privacy concerns when the web is such a public place.

From a broader strategic perspective, recent coordinated and stealthy attacks — including rifle shots to critical transformers in the Bay Area and Arizona, increasingly sophisticated, effective, and unprecedented cyberattacks, such as those in Ukraine — exposed troubling security gaps across the North American power grid and throughout the industrialized world.

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. More than 300,000 new malware detected daily is the new normal. Following the tragic events of 9/11, we have witnessed an increasing spectrum of threats, ranging from oil spills, to privacy concerns in an increasingly interdependent digital world, bio-warfare, cyber attacks, bombing attempts, food safety, natural disasters, personal privacy, safety and security. These threats have been in the spotlight while our national and international critical infrastructures face new challenges. The evolution of threats seems to be speeding up, and new vectors and modes of attacks emerge as we digitize without considering security and resilience as design criteria.

All progress comes with risk and is fragile. The very technologies that empower us to lead and create also empower those who seek to disrupt and destroy, making 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. We are becoming increasingly of these breaches, which are seen in the news almost weekly.

In summary, RISK is significant and issues abound.

Difficult Choices

More importantly, developing the tools that increase awareness and education about cyber threats is paramount. Yet it has been an ongoing challenge. Educating stakeholders and colleagues in the cyber-physical interdependencies has been difficult, as even distinguished members of the community who understand power systems well routinely minimize persistent, novel threats. Improving the sharing of intelligence, threat information and analysis to develop proactive protection strategies might improve the situation. This will include the development of threat coordination centers at local, regional and national levels.

To that end, TLI Director Dr. Massoud Amin led the work in this area (upgrading aging critical infrastructure – reliability, security and resilience – Technology, Policy and ROI) for the IEEE Task Force Report on priority issues in the 2014 Quadrennial Energy Review. His work included recommendations on what role the U.S. federal government might play in support of state and local efforts to aid energy, power and integrated utilities in increasing reliability, resilience and security.[1]

---

[1] U.S. President's Quadrennial Energy Review (QER) report, IEEE report to the U.S. Department of Energy and the White House for the nation's first-ever Quadrennial Energy Review (online http://www.ieee-pes.org/component/content/article/158-uncategorised/749-qer), particulaly pages 50-66 on "Asset Management and Security," August 2014. *And* "IEEE Joint Task Force on Quadrennial Energy Report (QER) Submits Final Report to the U.S. Department of Energy," *IEEE Smart Grid News,* October 6, 2014, http://smartgrid.ieee.org/resources/smart-

Like any complex, dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. While strong, centralized control is essential to reliable operations, this requires multiple technologies that are especially vulnerable when they are needed most: during serious system stresses or power disruptions. As security programs, such as CIP 5 are built and protections put into place, difficult choices will have to be made about how to handle a number of trade-offs, most of which we can *accomplish over the next five years, by addressing the following:*

1. **Outdated regulatory framework.** Split regulatory jurisdiction over the grid is inhibiting investment and modernization efforts. Bulk electric systems are under federal control, but individual states control distribution, metering and other aspects of the grid. Overlapping, inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships.[2] A new model for these relationships is required for infrastructure security. Additional regulatory reforms, such as the creation of a stockpiling authority, could obtain long lead-time equipment (such as transformers) based on the power industry's inventory of critical equipment, which decrease the probability an attack will substantially reduce grid functionality.

   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.

2. **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

grid-news/1164-ieee-joint-task-force-on-quadrennial-energy-review-qer-submits-final-report-to-the-u-s-department-of-energy.

[2] J. D. Bouford and C. A. Warren 2007. *And* FERC 2009.

working toward a common set of security requirements that will bring all electric sector entities up to at least a minimum level of protection.

3. **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.[3] However, pathways to cost recovery and making a business case for security investments and upgrades often pose challenges, since the benefits from those investments and upgrades are not always visible.

4. **Security versus efficiency.** The specter of future multi-hazard threats, including 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 and long-term technology development and deployment. Supportive public policy to aid cost recovery could greatly incentivize development of new business models and strategies.

5. **Centralization versus decentralization of control.** For several years, there has been a trend toward centralizing control of electric power systems. Regional transmission organizations were introduced in order to greatly increase efficiency and improve customer service. At the same time, terrorists can exploit the weaknesses of centralized control; therefore, a shift towards developing smaller and local semi-autonomous systems would seem to be preferable. 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 national objectives.[4]

6. **Wider grid integration and increasing complexity.** System integration helps move power more efficiently over long distances and provides redundancy to ensure reliable service, but it also makes the system more complex and harder to operate. The utility industry will need new approaches to simplify the operation of complex power systems and make them more robust in the face of natural or human-made interruptions.

7. **Dependence on Internet communications.** Today's power systems could not operate without tightly knit communications capabilities ranging from high-speed data transfer among control centers to the interpretation of intermittent signals from remote

---

[3] G. N. Ericsson, "Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1174-1181, July 2009. *And* T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber security risks assessment with Bayesian Defense graphs and architectural models," in *42nd Hawaii International Conference on System Sciences*, 2009, pp. 1-20.

[4] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," in *2nd Conference on Human System Interactions*, Catania, 2009, pp. 632-636. *And* I. Kotenko, "Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security," in *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Dortmund, 2007, pp. 614-619.

sensors. But due to the vulnerability of Internet-linked communications, protecting the electricity supply system will require new technology to improve the security of power-system command, control and communications, including both hardware and software.[5]

Question: 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***

1. **Critical regulatory issues currently being reviewed include, among many others:**
   i. How costs and benefits are apportioned to myriad stakeholders (and how that affects cost recovery for utilities);
   ii. Whether a microgrid relies on the distribution system (or transmission system) for backup and how that might affect reliability;
   iii. Whether and how to treat non-utility microgrid sponsors as utilities; and
   iv. Multiple possible business models for utilities offering microgrids.

2. **Metrics, best practices and roadmaps:** Establish workforce metrics 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.
3. **Select a lead organization, such as the U.S. Department of Defense (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 it can then 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.
4. **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 from which to develop survey results. For sales, forecasts, usage and other consumption related information, the Energy Information Agency (EIA) provides the best starting point.

---

[5] A. M. Giacomoni, S. M. Amin, and B. F. Wollenberg, "A control and communications model for a secure and reconfigurable distribution system," in *1st IEEE International Conference on Smart Grid Communications*, Gaithersburg, 2010 (submitted for publication). *And* W. A. Johnson, "A Utility program for enterprise security response," in *IEEE PES WPM*, Columbus, 2001.

5. **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.
    i. Determine what existing materials can be used to support the survey requirements, minimizing new data collection.
    ii. 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.
    iii. 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 scarce resources.

Our recommendations are:

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), 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. 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 a **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.
    - The 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 system**s 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) clearinghouse 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).

Looking where we are and what is likely to be ahead, I am grateful to several colleagues at the ASME, IEEE Smart Grid initiative, Energy Thought Summit (ETS), U.S. DOE, EPRI, EEI, NRECA, Munis, FERC, NARUC, NERC, PUCs, and elsewhere with insightful analyses and feedback from industry leaders. All these measures and more could be facilitated by more transparent, participatory and collaborative.

7. How will advances in technology (*e.g.,* artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

While advancements in areas such as artificial intelligence (AI), the Internet of Things (IoT), smart cities, interconnectivity IT (information technologies) and OT (operational technologies) can help automation, they'll pose additional nodes of entry, exploitation and failure modes if not engineered with security as a design criterion at every level. This includes hardware (including chip design), software, protocols, commutations and architecture.

As an example, cyber systems are the "weakest link" in the electricity system. Although vulnerability to attacks has been reduced, much remains to be done. Technology and threats are both evolving quickly, which adds complexity to the current cyber-physical system. In addition, there is often a lack of training and awareness by organizations (e.g., forgetting/ignoring the human factor in the equation). Installing modern communications and control equipment (elements of the smart grid) can help, but security must be designed into the system from the start, not glued on as an afterthought.

Increased emphasis at the state and federal level are combined with heightened needs for more innovative and improved ways to enable and protect economic growth and secure our nation and the world while preserving individual privacies, values and our way of life. So the key question is: **Can we build non-intrusive yet high-confidence tools, systems, processes, and laws that increase our security/resilience AND (it is an AND not an "or" option) preserve/extend our civil rights and liberties? Policymakers, industry leaders, engineers and key stakeholders should heed this advice to ensure the security, defense and resilience of these vital energy and commercial networks.**

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

ii. At the state or local level, including school systems?

iii. By the private sector, including employers?

iv. By education and training providers?

v. By technology providers?

Please see detailed responses and recommendations in the last 2 questions above. In summary:

Threat Situation is Changing:

- Cyber has “weakest link” issues
- Cyber threats are dynamic, evolving quickly and often combined with lack of training and awareness.
- All hazard, including aging infrastructure, natural disasters and intentional multi-pronged attacks

Innovation and Policy:

- Installing modern communications and control equipment (elements of the IoT, AI-enabled devices, smart grid and smart cities) can help, but security must be designed in from the start.
- Facilitate, encourage or mandate that secure sensing, “defense in depth,” fast reconfiguration and self-healing be built into the infrastructure.
- Protect the user from the network and protect the network from the user: Develop tools, standards and methods to reduce complexity for deploying and enforcing security policy.
- No amount of technology will make up for the lack of the 3 Ps (Policy, Process, and Procedures).
- Mandate security for the IoT, Advanced Metering Infrastructure, providing protection against Personal Profiling, guarantee consumer Data Privacy, Real-time Remote Surveillance, Identity Theft and Home Invasions, Activity Censorship and Decisions Based on Inaccurate Data.
- Wireless and the public Internet increase vulnerability and thus should be avoided.
- Bridge the jurisdictional gap between federal and state commissions on cyber security.
- Example: Electric generation, transmission, distribution, and consumption need to be safe, reliable, and economical in their own right. Asset owners should be required to practice due diligence in securing their infrastructure as a cost of doing business.
- Develop coordinated hierarchical threat coordination centers – at local, regional and national levels – that proactively assess precursors and counter cyber attacks.
- Speed up the development and enforcement of cyber security standards, compliance requirements and their adoption. Facilitate and encourage design of security in 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).
- Develop methods, such as self-organizing micro-grids, to facilitate grid segmentation that limits the effects of cyber and physical attacks.
- Security by default – certify vendor products for cyber readiness.
- Security as a curriculum requirement.
- Increased investment in the grid and in R&D is essential.