Massoud Amin: Good evening distinguished guests and colleagues. I am honored to …. 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 and targeted cyberattacks are on the rise with ever-evolving spectra of threats and more sophisticated adversaries:

Step back and reflect … Where have we been and what will the future hold? We are shaped by our time and have seen many emerging threats...

- From 1970s... Attacks in 1990s...
- Geo-strategic change ... Not new:
- Post-Soviet era, globalization, a highly interconnected world...
- Climate change,
- Gen. Wes Clark -- Serbia power grid in 1994

Y2K.... 9/11... …. 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, and cyber-attacks, to bombing attempts, food safety, natural disasters, personal privacy, safety and security… have been in the spotlight while our national and international critical infrastructures face new challenges. … Evolution of threats... all seem to be speeding up

Cyberattacks on cars connected to the Internet

Commercial aircraft: Connecting to live movie on the plane...

Who is doing the handshaking – are the aircrafts safe?

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. 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.

2. ***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.**

3. Third, 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. **BOTTOM LINE: The RISK is significant and the issues numerous and growing.** Answers to these challenges will undoubtedly take extended our discussions today.

(40 secs) It is a great honor for me to share the stage with Vice Admiral Tighe.

1. After graduating from the U.S. Naval Academy in 1984, then-Ensign Tighe was commissioned as a cryptologist.
2. Among her extensive list of accomplishments and accolades is her service as the first female commander of a numbered fleet in U.S. Navy history.
3. Today, as an expert in cyber warfare, she serves as the Deputy Chief of Naval Operations for Information Warfare and is dual-hatted as the 66th Director of Naval Intelligence.
4. After we hear her remarks, we'll conduct a brief Q & A session. Now, please welcome to Minnesota and to our stage, Vice Admiral Jan Tighe!

Backup Material

1) **Events of Last Weekend….**
2) **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 national security telecommunications and information systems (national security systems) against current and projected threats.**

I'll highlight that again: A comprehensive and coordinated approach is needed!!
This approach must include mechanisms for formulating policy, overseeing systems security resources programs, and coordinating and executing technical activities.

So the question is this – do we in fact have a comprehensive and coordinated approach?

Additional observations:

2a) Let's start by looking at the laws. Currently, Multiple laws and directives govern cybersecurity oversight.

- **Federal Information Security Management Act** of 2002
- **The Privacy Act**
- Executive Order 13587
- **National Security Directive**/NSD-**42**
- **Homeland Security Act** of 2002
- Homeland Security Presidential Directive **(HSPD) 7**: Critical Infrastructure Identification, Prioritization, and Protection
- National Security Presidential Directive **(NSPD) 54/HSPD-23**: Cybersecurity and Monitoring
- Office of Management and Budget (OMB) guidance concerning implementation of the Federal Information Security Management Act of 2002

- **The Federal Wiretap Act**
- The Stored Communications Act (SCA)

- FISMA: **defines a framework** for managing information security that must be followed for all information systems used or operated by a U.S. federal government agency in the executive or legislative branches, or by a contractor or other organization on behalf of a federal agency in those branches. This **framework is further defined by the standards and guidelines developed by NIST.**

2b) Is there a coordinated approach or "unity of effort" at the government level? Multiple departments and agencies have various Roles & Responsibilities:

- DHS
- DOD
- NSA
- OMB
- Department of Commerce
- NIST

DHS has the lead within the Federal Government

- to secure federal civilian executive branch information and communication systems. To that end they have recently published the "Blueprint for a Secure Cyber Future" in an attempt to unify the efforts…..
- to work with Sector-Specific Agencies and industry to protect privately-owned and operated critical infrastructure, and
- to work with State, local, tribal and territorial governments to secure their information systems.

But a series of recent articles seem to indicate a degree of angst associated with who does what:

- **The House Armed Services Committee (HASC) on Cyber Defense was quoted in an article titled: Forget DHS**

- **and in another – DHS, not NSA, Should Lead Cybersecurity, Pentagon Official Says**

--

3) The evolving spectrum of cybersecurity threats and countermeasures, which continue to improve yet poses novel threats, in several areas including:
    - Challenges confronting both the Public sector (incl. DOD) and consumers in the digital economy
    - Innovation (Internet of Things, healthcare, smart cities and other critical infrastructure areas)
    - Assured supply chains, products and services.

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, Russia and other adversaries.

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
- 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.

4) Other Somewhat Related Questions on a few potential smart cities and commercial areas:

1. What is your agency's definition of a "smart city"?
2. What are some of the needs and challenges for meeting this definition?
    a. Time-lines…? What are some blockers and accelerators?
    b. What are the business opportunities and ROI?
3. What are the top 3 desired outcomes in meeting this definition and why are they prioritized as such?
4. Who are the beneficiaries from a city becoming a "smart city"?
5. What are potential pilot projects to achieving these outcomes and what is the expected timeline for implementation.
6. When is it appropriate for government agencies (local, state and federal) to work together on smart city projects in the Twin Cities region? What are some examples … pilots ?
7. Last year, the Minneapolis-St. Paul area was selected to be part of the Transportation for America (T4A) Smart Cities Collaborative to explore how technology can improve urban mobility.
    a. From a city and county perspective, how will the goal setting and technical implementation be implemented locally and across the different agencies?
    b. Have pilots for this initiative been identified yet and if so, what are they, what is the timeline for completion, and what does success look like?
    c. If pilots have not been started, what are the likely first pilots based on discussions so far?

   d. Is there existing technology already in place that can be leveraged for pilots?

8. What role does the County have in smart city activity in cities outside of Minneapolis? Is there activity in any of these cities in implementing "smart city" technology and if so, how is it coordinated with the vision, outcomes and technology of Minneapolis-St. Paul?

9. When county and city agencies are looking at scaling projects beyond the pilot phase, what are some of the business models considered?

   a. If the model is a public/private one, how does one balance technology driving the project versus the city's desired outcomes?

   b. What are some of the differences in funding decisions for an IoT oriented project by a government agency versus a private sector investment?

10. **What are some of the technical and process infrastructure pre-requisites needed to become a smart city (e.g. data governance capabilities)?**

11. **What are some of the essential elements of a smart city platform? Have technical standards for these elements been established?**

12. **Any closing remarks, nuggets of wisdom … takeaways on pathways forward?**

Final:

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…

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 30 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 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 1450+ 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, our state and our nation 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.