Intelligent Infrastructure Congressional Briefing
House Science, Space and Technology Committee
Honorary Co-Hosts:
Rep. Lamar Smith, Chair, House Committee on Science, Space and Technology
Rep. Eddie Bernice Johnson, Ranking Member, House Committee on Science, Space and Technology

30 January 2018

Remarks by Nadya T. Bliss, PhD
Computing Community Consortium Council Member
Director, Global Security Initiative, Arizona Sate University

Good morning. It is an honor to be here, to join my distinguished colleagues, and to address this audience. I have spent the better part of the last two decades in defense and security focused R&D (at MIT Lincoln Laboratory and ASU). I am also a computer scientist. And it is clear to me that there has never been a more exciting time to be a computer scientist.

If you only take away one thing from my remarks, I would like it to be the following:

Security can no longer be an afterthought.

Investment in intelligent infrastructure creates much opportunity for our nation. As we build this new internet of useful things, we can build in security, trustworthiness, and privacy from the start. The cost of not doing so given the physical nature of these systems (vehicles, energy plants, bridges, and roads) would just be too high.

Embedded sensors and computing devices, algorithms, artificial intelligence, internet of things, autonomous driving vehicles – all of these present tremendous opportunity to transform and drastically improve resilience and adaptability, robustness and interoperability, accessibility and usability of our nation's infrastructure, as my colleagues have discussed or will discuss.

The complexity and interconnectivity of these systems – the interactions between autonomous vehicles and smart traffic lights, embedded sensors to anticipate repairs before they have caused harm, the ability to connect and leverage resources from remote and rural regions – all of this is what makes these systems of systems smart. It is the collection of the datasets in aggregate that has the potential to minimize traffic jams and car accidents, reduce maintenance budgets, and revitalize the economies of regions where the labor markets have drastically changed.

However, this moment of opportunity comes with significant responsibility. In itself, this responsibility presents an opportunity – we need to ensure that all these advancements are trustworthy, secure, and provide appropriate privacy guards.

For too long, security has been an after-thought in systems because functionality drives development - new functions are what people pay for. While the research community has made tremendous progress, vendors and service providers are slow to adopt these ideas, as evidenced by almost daily breaches and exploitation of vulnerabilities. These vulnerabilities have significant economic and societal impacts, as has been discussed in numerous congressional testimonies around the Equifax breach. Most recently, the hardware vulnerabilities – Meltdown and Spectre – have highlighted that most of our systems are vulnerable and there is no quick fix or patch.

Intelligent infrastructure will present attackers, be they individual cyber criminals or terrorists or nation states, with new opportunities to break systems. New research is needed to understand what these attacks might look like, and how they can be mitigated. Furthermore, sensors and components embedded in infrastructure will be hard to update or replace when compared to standard computing systems. So it is vital that we build security in from the very beginning.

To leverage this opportunity, it is vital that *all* research and development initiatives that support intelligent infrastructure, consider the following:

- **Trustworthiness: ensuring that the systems perform as expected**
- **Security: ensuring that the systems are protected from breaches**
- **Privacy: ensuring that the data and information collected are used as advertised with clear policy definitions for algorithmic accountability**

Not every initiative will require *new* research and development in trustworthiness, security, and privacy, but all should ensure that those three points are addressed.

The following are some specific recommendations.

As highlighted by recently identified vulnerabilities in computer architecture, **individual device security research at architecture and circuit level is necessary.** Given that the type of hardware that is likely to be used in intelligent infrastructure is either going to be low cost, mass produced (for example sensors) or highly specialized (for example, autonomous vehicles), these are going to require different techniques and approaches than the general computing devices. Similarly, **as these devices communicate, there is a need to research secure communication protocols for these devices** (for example, secure vehicle to vehicle and vehicle to infrastructure networks).

While the aggregate data available from all of these devices is likely to greatly improve infrastructure performance, **it is incredibly important to build in privacy protocols from the beginning.** Approaches need to be developed to ensure that the data is trustworthy

and reliable. Research in homomorphic computation, computation that allows you to operate on data while it is encrypted, has the potential to lead to privacy preserving algorithm development, but much work remains to be done.

Companies like Apple and the Census Bureau are already using differential privacy, or techniques for minimizing privacy loss while maximizing accuracy of queries. **This is a success story of transition of basic research, highlighting why these initiatives must continue to remain high priority.**

Another area that has recently emerged as requiring significant attention is accountability and explainability of algorithms. **As more decisions are made with the aid of automated systems, it is important to understand *how* those decisions are made.** Whether a decision is made to delay fixing a bridge or routing traffic around certain areas, these need to be justifiable, transparent, and ethical.

Many of the smart infrastructure initiatives are likely to be partnerships between public and private entities - for example, car companies partnering with cities, states, and the Department of Transportation. **How those entities engage with the data and what data can be used for what type of analysis are important topics to consider.**

With vast amount of new technology deployed throughout the country, there is tremendous opportunity and necessity for development of training programs, including ones focused on security and privacy. **Training modules could potentially be delivered online, presenting high tech job opportunities to areas where there previously were very few.**

Significant amount of excellent work is already ongoing.

Examples of existing programs include National Science Foundation's Secure and Trustworthy Cyberspace and Cyber-Physical Systems, Department of Energy's Cyber Resilient Energy Delivery Consortium, and Department of Homeland Security S&T Cybersecurity Division and Office of University Programs Centers of Excellence. Both Defense Advanced Research Projects Agency and the Intelligence Advanced Research Projects Activity under the Office of the Director of National Intelligence have made significant investments in cybersecurity, big data analytics, and image processing. Though not explicitly targeted towards intelligent infrastructure, many approaches developed under these programs are directly applicable to the challenges of processing massive datasets, developing explainable AI, and securing classification algorithms. Research and development funding in Department of Transportation is also vital as DoT is the agency that essentially owns this domain.

Not only is maintaining investment for these initiatives key, in most cases, additional investment would greatly accelerate implementation and deployment of intelligent infrastructure and do so in a safe, secure, and responsible manner.

One particular area that needs increased investment is interdisciplinary research. Efforts in security and privacy require not just computer scientists, but social scientists, humanists, legal experts – just to name a few.

Finally, an area that requires attention is both research and implementation of policies in context of risk and security of intelligent infrastructure. For example, if the software being used across sensors is hacked and a bridge collapses or the power grid shuts down causing massive outages, who has the responsibility? These and other questions highlight the need for an ongoing dialogue between the R&D community and the policy community.

Opportunity to brief you today is an excellent step in that direction. We very much appreciate the time and happy to discuss any and all items further if appropriate.