Senate Commerce, Science, and Transportation's Field Hearing
"The Race to 5G: A View from the Field."
October 12, 2018
Dr. José-Marie Griffiths, President
Dakota State University, Madison, South Dakota
Written Testimony

5G Networking – From the Internet to the Cyber Universe – the Cyberverse
From the Information Superhighway to an Ocean of Collaborations

A shift
from driving data location to location
to living, working, and playing in an environment of technology-infused interactions and collaborations

INTRODUCTION

This hearing is asking those of us testifying to address three topics:

1) Existing barriers to broadband deployment on the horizon of next generation wireless technology deployment,
2) ways to encourage investment in next generation communications services, and
3) ways to streamline broadband deployment siting.

I believe the best way to address all three of these issues is as follows:

1) Invest the resources necessary to **build widespread understanding and knowledge** of what 5G and the Cyber Universe are and why they are so important to the economy, security, and quality of life for the United States in both the near and far future;
2) **Engage cyber security professionals** in every aspect, from the ground up, of the creation of a 5G and Cyber Universe testbed such that the model U.S. 5G environment is not only effective and efficient, it is also safe and ensures the privacy and democratic values to which we in the U.S. are committed; and
3) **Rapidly create a publicly/privately-funded partnership to build and deploy a real-world 5G and Cyberverse testbed** across a geographic area in the U.S. that contains a cross-section of U.S. population clusters and organizations, geography, climate, industries, and existing technologies, to explore, troubleshoot, and establish best-practice models for the technology as well as the policies and governance required to support 5G development and deployment across the country.

I. BUILDING KNOWLEDGE AND UNDERSTANDING OF 5G AND THE NEW CYBER UNIVERSE - What are 5G and the Cyberverse and why should anyone care?

In order to build widespread understanding and knowledge of what 5G is and why it is so important to the economy, security, and quality of life for the United States and its citizens in both the near and far future, we must first be clear about what is 5G and what is the new Cyber Universe – the Cyberverse – it will enable.

We have become accustomed to our technology becoming, ever rapidly, faster and more capable. We understand that most of our computers or smart phones or networks have a half-life shorter than most pro football coaches (their average is about 3 years). It's hard to be excited or very energized by – or put a lot of investment into – some new technology that we anticipate will lose its "wow" factor predictably and

soon. The "yawn factor" runs deep these days in the general public's – and even much of leadership's - reaction to calls from techies to embrace yet another supposed new breakthrough technology with some new strange name, like "5G and the "Cyberverse."

5G is NOT just another iteration of what has come before. In reality, calling 5G the fifth generation, just as 1G was first generation, 2G was second generation, etc. is a misnomer. 5G is a totally new and radical approach, not just to telecommunications and networking, but to how we live, work, and play in the cyber universe.

A) THERE IS TROUBLE ON THE INFORMATION SUPERHIGHWAY

As amazing as the Internet is, there is trouble on the Information Superhighway. We are facing multiple problems in our present cyber environment, including availability/capacity, reliability, speed, responsiveness, interoperability, security, energy efficiency, expandability, and the flexibility to support the complex problem-solving processes that the complex problems of the 21st century require.

i) Travel on the Internet is not optional – network connectivity and technology access are essential community goods

Today, the technology an organization uses – and how effectively it uses it – is just as essential to its success as its reason for existence – the service or product it generates. There is really no significant activity in this country that does not depend heavily, and often for its very existence, on technology, telecommunications, and computer networking. From finance to agriculture to manufacturing to healthcare to government to entertainment, the cogs of our modern society move by the power of cyber.

All this cyber use means that the traffic on the Information Superhighway is increasing at a rate that is difficult to grasp. According to a study by Cisco, Internet traffic is on target to increase by 25% every year between 2016 and 2021. We are also on trend that by 2021 the number of devices connected to IP networks will be more than three times the global population, at the equivalent/per capita of 3.5 networked devices for every man, woman, and child on the planet. Between 2016 and 2021 we will have added 10 billion devices online, from 17.1 billion in 2016 to 27.1 billion in 2021. It would take more than 5 million years for one person to watch the amount of video that will cross global IP networks each month in 2021.[1]

ii) Traffic jams are increasingly common - capacity constraints are creating availability, reliability, speed, and responsiveness problems

All this traffic is causing global-sized traffic jams. The bottom line is that we don't have enough lanes on the Information Superhighway to accommodate everyone and everything that wants to use it. And we don't have enough available real estate on the present routes, i.e. the presently used radio spectrum bands, to add more lanes, technically called bandwidth. The result is the cyber world matches L.A. traffic at rush hour in the physical world. And without the required capacity on the Highway, availability, reliability, speed, and responsiveness fall off exponentially.

Practically, at the busiest times of the day cyber users may find that they are totally unable to even get on the Internet – there are simply no lanes available for them, there is no more bandwidth available for their transmissions. We have all had the experience of watching the spinning ball on our monitors with increasing frustration as we try to get on the virtual Highway. If the traffic jam and lack of bandwidth is really bad, the system may just give up trying. An error message will pop up on our

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

screens saying that the connection "timed out" and we have to click our mouse or enter a command to try afresh to connect. Once we do connect, depending on how our connection is routed, if we hit a place where the traffic overwhelms the available lanes, the available bandwidth, we may be knocked off the virtual highway altogether and, from our virtual 'ditch,' have to try yet again to get back on the highway into a lane.

All this congestion means that we cannot rely on how long any transmission will take. Latency, the delay between an action taken on my computer and being received at another device, is critical in more and more applications. In the early days of the Internet, trying to 'crystal ball' the future, developers attempted to guess at what might be possible if we had this ubiquitous resource to move information around. At the outer edges of that imagining, people suggested things like remote surgery with a physician able to operate robots in an operating room in a rural area, providing life-saving care to patients who do not have access to that specialized surgeon's skill and expertise. They envisioned collaborations involving real-time meetings with hundreds of thousands of people interacting with each other using the same application on their various devices, all at one time, for example following a natural disaster or in a military operation. The reality is that we do now have the technology to do these tasks and many more. However, the increasingly crowded bandwidth of the Internet and the resulting traffic jams not only impact availability and reliability, speed and responsiveness have also deteriorated. The movement of the surgeon's hand tying off a bleeding blood vessel must be transmitted in milliseconds to the robot device actually carrying out the action inside the patient's body. Network latency cannot be an issue.

And the amount of information to be transmitted is more and more extensive and detailed, which also is going to require more lanes of the highway. A less dramatic but economically significant example is with supply chain management. U.S. manufacturers are dependent on supplies coming from around the world on a predictable schedule. Being able to prepare for a shortage, for example, of the raw materials to make a car's dashboard, can save or cost an automaker thousands of dollars, enabling them to shut down or repurpose a factory line. It's not enough for the ship carrying those materials to have a system with sensors that lets the captain know that a part has broken down inside the engine. Now it is possible and economically necessary for that engine to have sensors that can predict that a part is close to breaking down, which sends a message to a system that figures out when it will fail entirely, which then sends back a message to shut down the engine to save damage to other parts while sending an alert to the repairman as to what needs to be fixed and, simultaneously, notifying a supplier thousands of miles away and multiple steps down the supply chain that the car dashboard factory line is not going to have the parts on time. This scenario is entirely possible, but the present telecommunications system does not have the bandwidth to accommodate this and the other millions of scenarios in multiple industries.

iii) Too many people have keys – and they're all different – maintenance, security, and interoperability in the present technology environment are dependent on millions of (non-techie) people being technologically savvy and responsible

We are also now struggling with a high level of technology knowledge required of even the most casual user. It's one thing when you only have very smart technology people using the network and sharing information. It is another thing when you have millions of people doing that, an enormous number of whom have no interest or ability to, for example, keep their passwords private and change them often, or upgrade software on their multiple devices every time another security vulnerability is identified or a company has decided to upgrade or expand the features available in their applications. In addition, the responsibility for getting all of our various devices connected to the Information Superhighway falls on each of us individually. And often the way to do so is different for each device – smartphone, computer, tablet, gaming console, etc.

In addition, I think most of us without thinking about it, have all taken on an enormous time-drain of overhead in obtain, maintain, and use our ever-increasing number of devices – a smartphone, a tablet, a laptop computer, a desktop computer, now rapidly being joined by a TV, various kitchen appliances and/or a smart speaker like Alexa. There is at present a serious contrast between, for example, electricity and technology networking.

Electricity is generally pretty invisible. Except when it goes out, most of us, I don't believe, spend much time thinking or dealing with electricity. We push a light switch – in our kitchen, in our office, in the restroom at the restaurant – the electricity connects and the light goes on.

This is not the case with our "smart" phones. In order for my phone to work in my kitchen, I have a cable coming into my house connected to a cable modem, which I have to set up with a user name and a password. If the network goes down or becomes disconnected, I will have to reset and re-enter the cable modem user name and password.

The cable modem talks to a Wi-fi router sitting on a bookshelf in my living room, which also has a network name and password. When the cat knocks that device over and it becomes unplugged, I will also have to plug it back in and re-enter that network name and password. When I brought my cell phone home for the first time (or when I get a new one) I have to go into settings on that phone, have it find my home network (out of an amusing list of network names of my neighbors' Wi-fi networks), and use the correct user id and password to get it connected to my Wi-fi and, ultimately, to the Internet, where I likely also have to use various different user ids and passwords to get into various sites to access any information I might have online, like my bank account, or be able to purchase something from an online store.

Going to check my balance in my bank account first thing in the morning, I discover that the before-school teen crowd in my neighborhood has taken over the network bandwidth to check in with their friends as to what they're going to wear that day. It takes so long for my typed-in request to get to the bank website that they consider I've been on my account so long that it's a security risk and they have logged me out. Network latency has hit again. And I haven't even left the house yet…

Heading out for work, I lose my home Wi-fi connection by the time I'm in the garage, where I have to wait for my phone to (hopefully) connect to my cell network (which also initially required a user id and password) and then via bluetooth to my car's audio system. On the way to work, depending on the coverage of my provider's network, my phone may or may not stay connected during the conversations I'm trying to have while enroute. When I arrive at work and go up to my office, my phone once again has to switch to the office Wi-fi (which at some point – and perhaps now and again must be repeated – requires yet another user id and password). I get to the office and login in to my computer (yes, another user id and password) and an alert comes up telling me that someone has discovered yet another security vulnerability in my operating system and I must install an update immediately. Installing that update requires my going to a website (where I have to login with – yes – another user name and password), download the software and install it, which takes three attempts because everyone else just got to the office and they are also trying to download the software and so I keep getting logged off the software download site. Once logged on, I send to a coworker a copy of a file that I worked on last night on my home computer. He sends me an email back saying he can't read it, because I have a different version of the software on my computer than he has on his.

The present networking and computing configuration has put the maintenance, interoperability and most concerning, security of our cyber endeavors in the hands of millions of individuals with minimal knowledge, understanding, and unknown values.

iv) People no longer want to ride only in their own vehicles – 21st century problems require fluid multiple interactions for people and technology

At the same time as we're hitting a brick wall with our existing technology and networking approach, users are increasingly demanding far more than just access to information. The complex problems of our 21st century world require a more complex and fluid ecosystem of participants, machine and human. People don't want to just access or give information, they want to interact with it, to be immersed in the process of its creation as much as its dissemination and extension. And they don't just need to interact with it by themselves, they need to collaborate with multiple others in a three-dimensional environment where they can tap into people to people, machine to machine, and people to machine interactions – more like an ocean than a highway.

In addition, the machines are becoming smarter and smarter. The last 10 to 20 years have seen phenomenal growth in artificial intelligence and machine learning functionality. Computers are now able to take millions of pieces of data, identify predictive patterns and knowledge, and then use those results to inform and direct further processing and analysis. This is allowing humans to leapfrog over literally years of research to ask new questions in new ways, leading to the creation of new tasks for AI and machine learning machines to work on. However, AI and machine learning require almost instantaneous access to enormous amounts of data and need to transmit enormous amounts of data. Today's crowded Internet cannot accommodate the speed or density of communication that are required for these new functions to work effectively.

B) 5G AND THE CYBER UNIVERSE – the Internet is fixable

As impressive as today's Internet is, it is clear that our present telecommunications and cyber environment has major problems in

- limited bandwidth;
- unacceptably long latency, slow speeds, and inadequate reliability;
- inappropriate dependencies on users for security and maintenance,
- interoperability chaos, and
- inability to accommodate the multidisciplinary, multi-agent processes required of people to people, people to machine, and machine to machine interactions for 21st century endeavors.

i) How 5G will move us from the Information Superhighway to the Cyber Universe

Bandwidth, latency, speed reliability

5G deals with bandwidth and latency in a new way, resulting in orders of magnitude improvements in cyber speed and reliability.

The radio spectrum is broken up into bands, each with different features as you move up into higher frequencies. Our existing telecommunications systems work on certain bands of frequencies. 5G will run on a new "high-spectrum band", which uses higher frequency signals than previous generations of telecommunications. The new band will be much less congested than at present because there are many more frequencies available in higher ranges. These high frequencies are great for a number of reasons, one of the most important being that they support a huge capacity for fast data. Not only are they less cluttered with existing cellular data, and so can be used in the future for increasing bandwidth demands, they're also highly directional and can be used right next to other wireless signals without causing interference or crossover.

This is very different from 4G towers that fire data in all directions, potentially wasting both energy and power to beam radio waves at locations that aren't even requesting access to the Internet. 5G also uses shorter wavelengths, which means that antennas can be much smaller than existing antennas while still providing precise directional control. Since one base station can utilize even more directional antennas, it means that 5G will support over 1,000 more devices per meter than what's supported by 4G. Traffic jams, and the resulting crashes and slowdowns that contribute to today's lack of connection reliability will be a thing of the past once 5G is deployed. Given that the Internet of Things is going to move us into an almost unimaginable number of devices on the network, we need that capacity and speed yesterday.

With 5G, for example, when a user makes a request from their phone, the network will respond about 10 times faster than the blink of an eye. (That is, network response times will be approximately 1 millisecond.) Importantly, this is below the human threshold to even detect a delay! To the physician's hands sending signals to the remote robot, it will seem to the doctor that he and the robot are moving the scalpel at exactly the same time.

Security, maintenance, interoperability

One of the goals of 5G is to make our networking connections as invisible and requiring as little of our attention as electricity does now. 5G is designed to have everything connected to everything else, and to have all that connectivity taken care of and managed not by each individual user but by systems and processes in the Cloud.

For example, with 5G, the network follows a user through "cells" – geographic areas of connectivity. That cell of connectivity will no longer depend on a certain type of connection, for example Wi-Fi or cable. The network will seamlessly connect together all of the various cells provided by various technologies. Whether connectivity is being provided by a cellular network or a cable modem or a "small cell" device on the telephone pole outside their window will be of no concern to the user and will require no action on their part. In this heterogeneous but cohesive network, cells will assess the needs of each user's device and route it to the most efficient services regardless of where location. There will continue to be larger cells, with broad coverage, but other areas, for example, a college campus, will be covered by small cell technology hung on lamp posts or the roofs of building, and, in new buildings, possibly even inside the bricks in the wall. But none of these different connections will require every individual user to enter a user id and password as their connection is moved from cell to cell.

For example, algorithms in the network will determine how fast a moving device is travelling and what it's networking needs might be because of that. An autonomous vehicle might be connected to a large or macro-cell, such as a large cellular tower, so that it stays connected without having to be shifted from cell to cell as it travels over a long distance. However, students walking across campus, texting on their smart phones can connect to smaller cells with less coverage, as the connections can easily be transferred to the next small cell as needed, so quickly that the student won't even notice.

Everything will be connected to everything all the time, just like electricity. Once the connection is there it stays connected. And if it goes down, when it comes back up, once again everything will be connected to everything else without any intervention on the part of users.

An example of the difference in this approach can already be seen in our K-12 schools, many of which have moved from tablets or laptops for their students to Chromebooks. What is the difference? For schools, which often need to have many hundreds of devices to serve their students, teachers, and staff, a huge difference is in tech support. A tablet or laptop has an operating system (OS) on it, as well as applications. When there is an update to either the OS or any of the apps, that update has to be installed on each device. While school networks often do have programs that will update multiple machines at the

same time, some IT support person still has to ensure that all the devices are charged or plugged in and on the network and not being used at the time to run that program and that no one happened to take their machine home the night tech person is installing the upgrade. And that some user didn't go rogue and install some out-of-the-ordinary app on their machine that collides with the new OS or software upgrade.

Chromebooks update themselves automatically both for OS upgrades and application upgrades. There are no applications on Chromebooks – they connect to the Internet and use applications in the cloud. If an application needs updating, it is updated in the Cloud and the next time the students go to that app, they are automatically connected into the new version.

One of the features of 5G is to move to the Chromebook model rather than the tablet or laptop computer model. It is a shift away from our devices - hardware and what is included and runs on a particular device - to having all the technology we need to use running in the Cloud. The device we use to connect to the Cloud becomes almost unimportant. Incompatible files caused buy only having access to a certain old version of a software application would be a thing of the past. How many times have we gone to show someone something on our phone and say "oh, I can't get that on my phone – I'll have to show it to you on my computer." It used to be that children would say "my dog ate my homework." Today it is "my computer crashed and I couldn't print it out" or "my brother spilled orange juice on my laptop and fried my file." New excuses will be required with 5G – that homework will live in the cloud and be available from anywhere on any device.

With zero perceived delay in access, even for those large files, 5G will change the economics of technology expense within an organization. The faster, low latency, reliable connections will make it more sensible to move expensive cyber storage and processing into the Cloud, which will require much simpler, less expensive, lower-maintenance devices in the hands of users.

In addition, by moving the bulk of processing and storage into the Cloud, the energy demands of user devices will drop as well. It will be possible for smartphones, for example, to have batteries that last weeks or even months, given that the only processing required on that device is to make a connection to the network and then the Cloud. Medical implants will be able to function for decades without having to be removed or upgraded, since only maintaining a connection to the network will require very little battery use.

ii) An immersive efficient cyber universe of interactions

When bandwidth, reliability, latency, security, maintenance and interoperability are no longer constraints, it will be possible to migrate to a fluid immersive cyber universe of the people to people, people to machine, and machine to machine interactions required for 21st century endeavors.

Analysts predict that by 2020, each person in a developed country will own and use about 27 connected devices. These will range from existing technology, such as smartphones, tablets and smartwatches, to refrigerators, cars, augmented reality glasses, and even smart clothes. Some of these devices will require significant data to be shifted back and forth, while others might just need tiny packets of information sent and received. The 5G system itself will understand and recognize this and allocate bandwidth respectively, thereby not putting unnecessary strain on individual connection points.

II. CYBER SECURITY MUST BE BUILT IN FROM THE GROUND UP – and why it is important the U.S. get to 5G first

A) Cyber Security Professionals

We must engage cyber security professionals in every aspect of the development of the U.S.'s 5G system. such that this country's 5G environment is not only effective and efficient, it is also safe and ensures the privacy and democratic values to which we in the U.S. are committed.

With great power comes great responsibility, and that has never been more true than with the development and deployment of 5G and migration into the Cyberverse. 5G is what will make it possible for us to move into the Internet of Everything (IoE). However, every time we connect a new device to the network we also potentially open up a new set of vulnerabilities. Presently companies are racing to make their devices, from crock pots to lawn mowers, IoE-ready. In the absence of instructions and requirements, cyber security tends to be the last consideration of most of these manufacturers. The U.S. is sorely lacking right now in standards and best practices for security to be built into IoT devices, or the software that can easily be installed as part of the basic features of any device.

The U.S. is presently seriously under-resourced in cyber security professionals. The vast majority of the cyber security professionals we do have are over-extended trying working to mitigate and remediate existing Internet attacks, which multiply faster than the proverbial rabbits. However, it is critical that the U.S. ensure that a network upon which every activity in this country is dependent is developed in such a way that vulnerabilities are reduced as much as possible, and that the U.S.'s 5G and Cyberverse cyber security expertise proceeds in step with the development of our national 5G networking capability. This is one area that is of such common concern and serves every individual and enterprise in the country that it would be appropriate and likely necessary for the federal government to provide the upfront investment in the recruitment, education, and deployment of cyber security professionals in 5G development.

B) Why we must get to 5G first – and why we are falling behind China

According to a study released by Deloitte Consulting, a top industry consulting firm, this past August 2018, the United States is losing the race against China to develop and deploy a nationwide 5G network. For a long time, the U.S. led in telecommunications and networking. As FCC Commissioner Jessica Rosenworcel has said, the U.S. has 5% of the world's population but we have over 50% of the world's 4G deployment. The smart phone revolution and the application economy started in the U.S. and we have reaped the rewards of that leadership position. Other countries have decided they are not going to let that happen with 5G.

There is more at stake here than just prestige. The National Security Agency has stated that if China dominates the telecommunications network industry it "will win politically, economically, and militarily." Michael O'Reilly, one of the U.S. FCC commissioners has stated that he believes if the U.S. loses the race to 5G it will mean that the nation will be dictated to by foreign powers, many of which can't be fully trusted, don't believe in capitalism, don't believe in freedom, don't believe in fair play, don't believe in the role of the individual over the government, and rebuke American leadership."

Deloitte's report also states that since 2015 China has outspent the U.S. by $24 billion in 5G infrastructure. China has built 350,000 new cell sites, while the U.S. has built fewer than 30,000 in the same time-frame. The U.S. mobile carriers' industry association, CTIA, estimates that the number of cell sites in the U.S. must more than double from about 325,000 to 800,000 for 5G to be deployed. Deloitte's report noted that China plans hundreds of billions of dollars in 5G-related spend and suggests that "China and other countries may be creating a 5G tsunami, making it near impossible [for the U.S.] to catch up."

In addition to the concerns of national security, there is no question that the first country to effectively deploy 5G and the Cyber Universe will also reap enormous macroeconomic gains. Given the increased capabilities of 5G and the Cyberverse, companies that develop and are designed to take advantage of those capabilities will quickly become global leaders. There is also something called the "data-network effect," in which early leadership in new markets translates into more users who generate more data that, in turn, helps improve services and attracts more users. The first to deploy 5G and the Cyberverse in a real-world setting will also be the country to understand the strengths, weaknesses, opportunities, and threats related to the new technology.

III. WE NEED A PUBLIC/PRIVATE PARTNERSHIP TO BUILD AND DEPLOY A REAL-WORLD 5G AND CYBERVERSE

A) What we need

The United States needs to rapidly create a publicly/privately-funded partnership to build and deploy a real-world 5G and Cyberverse testbed across a geographic area in the U.S. that contains a diverse cross-section of population clusters and organizations, geography, climate, industries, and existing technologies. This entity will make it possible to explore, troubleshoot, and establish best-practice models and tools for 5G and the new Cyberverse, as well as the policies and governance required to support similar development and deployment across the United States.

5G and the new Cyberverse is clearly critical to the economic, safety, and quality of life future for this country. But there is a lot we still don't know and won't know until we actually fully deploy and use a 5G network and a Cyberverse. And we need to do it quickly.

A big issue in the U.S. is finding a workable model for municipalities, states, and the nation, along with private industry, to work together to integrate the multiple networking components and resources it is going to take to achieve 5G. In an authoritarian country such as China, those are nonissues, and so they are moving very rapidly through that process. We can be successful in this work in the United States, still maintaining our respect for the rule of law and regional rights, but we need a model to do so. To develop that model, we need to develop and deploy a test 5G network in an area that has multiple types of communities. A model that will work in a large city will likely not work the same way in a rural area or a small town. More than 85% of cities in the U.S. are small, under 10,000 people. If we are going to reach ubiquitous 5G, we have to develop a model that works in more than just urban areas along the two coasts. However, at present the telecom companies are concentrating only on those two areas, seeing them as the "low hanging fruit" where they can make the most money quickly. Only 15% of the U.S. population lives on the west coast, and only 17% in the northeast, which means that 68% of the country does not live in the areas where U.S. telecoms are working to develop 5G. It is going to take federal leadership and investment to ensure that more than two-thirds of the country are not bypassed by the next technological revolution.

B) SD5G and the SD CYBERVERSE

South Dakota is now working to become the first state in the nation to develop and deploy a state-wide 5G network and Cyberverse. We believe that our state has the characteristics and resources that make it the ideal place for such a project. We are eager to move forward to create for the nation a model of how to address the various challenges of this transformative approach to the delivery and use of technology.

An American model for 5G and Cyberverse development and deployment must develop best practices that integrate the needs and particular characteristics of multiple:

1. Cyber security demands, software to hardware, end user through the Cloud

2. Technologies – small cell, large cell, fiber, etc.
3. Enterprises – education, government, agriculture, manufacturing, health care, transportation, etc.
4. Population clusters and types – from urban to rural, with special focus on making sure the "last mile" and the "last inch" are as connected as the first and reviving "main street" through migration to 'smart cities'
5. Governmental organizational structures and concerns – city, county, state
6. Geographies and climates

1) Cyber security demands, software to hardware, end user through the Cloud
South Dakota is home to Dakota State University (DSU) in Madison, South Dakota. DSU is part of a state-wide regental system of six public universities. The DSU started in 1881 as a teachers' college to serve the growing educational needs of the Dakota Territories and over time grew into a comprehensive university. In 1986, a remarkably prescient South Dakota state legislature re-missioned DSU to add to these roles an augmented and specific focus on technology-infused and technology-intensive degree programs and R&D.

Today DSU is one of the leading cyber security universities in the country, with four Center of Academic Excellence designations by the U.S. National Security Agency and Department of Homeland Security, in cyber education, operations, and research. The Beacom College of Computer and Cyber Sciences has a breadth and depth of cyber degrees, associates through doctoral, unmatched by any university in the country, its graduates at 100% placement, either in a professional position or a top graduate school. DSU also has the largest cohort in the country of the National Science Foundation's CyberCorps Scholarship for Service program, where in exchange for scholarship support after graduation individuals serve in a state, federal, or tribal organization for the same number of years they received the scholarship. Dakota State is also home to the Madison Cyber Labs. The MadLabs is a prolific collection of public/private partnerships in research, scholarship, economic development, and policy development clusters organized around expertise and technology application in specific enterprises. DSU has experts exploring and working with leading edge technologies in a wide range of disciplines, from health care to adaptive technology for individuals with disabilities, from digital forensics to cyber security for the financial sector, and more. There are presently 14 clusters, and a new facility, funded by a private/public partnership, will open in 2019 to provide centralized and collaborative space for the MadLabs. Because DSU is part of the state-wide comprehensive regental university system, it is integrated into a rich fabric of disciplinary experts and exploration at the other five universities with their various emphases, from agriculture to law, from the medical school to mining.

South Dakota is thus developing and will be deploying our 5G and Cyberverse solutions with the professionals and resources of DSU's robust cyber security environment interwoven into every decision and solution. We continue to see the enormous cost to public and private safety and security when cyber security issues are ignored or left out of technology solutions. One only needs to consider the recent issues facing Facebook over the last few years to understand that we must never again consider cyber security a lower level "add on" to our technology innovations and solutions.

2) Technologies – small cell, large cell, fiber, etc.
South Dakota has been remarkably energized and diversified in pursuing and taking advantage of networking and cyber innovations and technologies. One of the reasons for this is that with a smaller population, the state can be remarkably agile in making decisions and implementing change.

In addition, the state has a wide cross-section of needs in its population that are representative of the wide cross-section of needs across the country. South Dakota has urban (e.g., Sioux Falls) and rural populations, and a large collection of typical "small town U.S.A." communities. The state continues to have strong concerns and is constantly looking for quality-of-life improvements for its Native American population, which for the most part continues to face poverty, physical and mental health illness, and a lack of socio-economic opportunities. Because of the wide geographical distribution of population, many physical solutions to issues in education, healthcare, transportation, business, development, etc. turn out to be cost-prohibitive and impractical. Early on, as the State legislature's 1986 commissioning of DSU illustrates, South Dakotans recognized that computing and cyber had more potential to provide solutions to its challenges than the models developed and implemented in more geographically dense areas of the country. South Dakota is by no means alone in this respect. As mentioned before, 85% of U.S. towns have populations under 10,000 people, and 68% of the country's population does not live in the primarily urban or population-intense northeast or west coast.

Thus South Dakota has already taken initiatives to create the foundation of multiple networking technologies that will require integration to deploy 5G and the Cyberverse. The state already has a number of areas that have deployed small cells, and a number are under development. Sioux Falls and Brookings, two of the state's larger cities already have some small cells deployed. Dakota State University is working in collaboration with the City of Madison to deploy a city-wide small cell system in the next year. The state is connected to the Internet2 high-speed fiber background through the REED Network.

One of the most innovative new networking technologies has emerged from Google's Project Loon, an effort to find a new way to provide Internet access to rural and remote areas. The company that emerged from the R&D project uses high-altitude balloons placed in the stratosphere at an altitude of about 18 km (11 mi) to create an aerial wireless network. The balloons use patch antennas – which are directional antennas – to transmit signals to ground stations or LTE users. Some smartphones with Google SIM cards can use Google Internet services. The equivalent of the "base station" that talks directly to devices is carried in the balloon (adding new meaning to the idea of technology in the "cloud"). Users of the service connect to the balloon network using a special Internet antenna attached to their building. The signal travels through the balloon network from balloon to balloon, then to a ground-based station connected to an Internet service provider (ISP), then onto the global Internet. The system aims to bring Internet access to remote and rural areas poorly served by existing provisions, and to improve communication during natural disasters to affected regions. It was named Project Loon for 2 reasons: one was that even Google itself found the idea of providing Internet access to the remaining 5 billion unconnected people in the world an unprecedented and "loony" idea, and 'loon was a short-hand for the "balloons."

It turns out that South Dakota is a significant partner in the Loon technology, through the company that makes the highly sophisticated balloons, Raven Industries, Inc. Established in 1956 to make high-altitude balloons, Raven was launched by a group of General Mills employees, including General Mills High Altitude Research division employee Ed Yost. Yost picked Sioux Falls for its favorable wind conditions and over the years the company has focused in on its precision agriculture, engineered films, and Aerostar divisions. The U.S. military and other government agencies are among its clients. The balloons are superpressure balloons filled with helium and stand 49 feet across and 39 feet tall when fully inflated. They carry a custom air pump system that pumps in or releases air to ballast the balloon and control its elevation. A small box weighing about 22 lb containing each balloon's electronic equipment hangs underneath the inflated envelope. This box contains circuit boards that control the system, radio antennas and a system to

communicate with other balloons and with Internet antennas on the ground, and batteries to store solar power so the balloons can operate during the night. Each balloon's electronics are powered by an array of solar panels that sit between the envelope and the hardware. In full sun, the panels produce 100 watts of power, which is sufficient to keep the unit running while also charging a battery for use at night. A parachute attached to the top of the envelope allows for a controlled descent and landing when a balloon is ready to be taken out of service. In the case of an unexpected failure, the parachute deploys automatically. When taken out of service, the balloon is guided to an easily reached location, and the helium is vented into the atmosphere. The ground stations use a Ubiquiti Networks 'Rocket M5'radio and a custom patch antennae to connect to the balloons at a height of 12 miles. The balloons are equipped with automatic dependent surveillance broadcast and so can be publicly tracked along with other hot air and weather balloons.

Those who think of South Dakota as home to vast farms on the Plains, buffalo and cattle ranches stretched across the buttes, the lifestyle of Little House on the Prairie, and Native American heritage should be aware that these days the state is also home to impressively sophisticated technology development and cyber innovation. Silicon Valley or Boston's metropolis are rapidly being matched by a technology revolution in the center of the United States. DSU's cyber security and Raven's Loon system are matched by multiple enterprises across South Dakota working at the vanguard of precision agriculture, robotic manufacturing, and distance-delivery health care, among others.

This multifaceted foundation of expertise and deployed technologies is making it possible for South Dakota to move rapidly in the development and deployment of SD5G and the SD Cyberverse. The only constraints at present are garnering the investment needed to move as rapidly as we are able to. We understand the national security and economic impacts of the United States achieving working and workable 5G and Cyberverse models before those countries whose development of these technologies will likely not be in our best interest or to our profit. South Dakotans long learned how to overcome obstacles and turn dry ground into fertile fields, and our efforts in cyber are determined to be comparably fruitful.

3) Enterprises – education, agriculture, manufacturing, health care, etc.

South Dakota, especially over the last century, has developed a remarkably diverse business and industry environment. In every area, often due to the particular challenges of rural areas and difficult geographies, technology development and use is key to the state's economic development and health.

a) Education

5G and the Cyberverse will be especially transformative in terms of education. The South Dakota university system launched some of the very first online courses, and, for example, DSU's Internet-based degree programs reach students across the country and around the world.

Technological advances have already moved many rich digital resources far beyond the physical confines of the classroom and into the hands of learners. 5G and the Cyberverse will enable a learning model that will be an international, immediate, virtual, and interactive environment. It will make it possible for teachers and students to learn and interact in much different ways that we do today. The new model will be learner-centric, skill-centric, on-demand and personalised, which will in turn improve student development in the areas of critical-thinking and collaborative learning.

5G and the Cyberverse will create a network capable of transferring our tactile communication from one location to another, from one device to another. This will make

it possible to move beyond today's online teaching focus of content and information delivery to the ability to train students in hands-on skills, what some are calling manual handskill delivery.

Virtual reality (VR) has initially been developed primarily by the entertainment industry, but with 5G networking in the Cyberverse VR has tremendous potential and relevance for education and training. For example, with a VR application, students could not just learn about the seven wonders of the world, they could visit them and explore on their own, at their own pace and direction the sights and sounds that make those locations especially remarkable. They could stop and examine those things of greater interest to them, and immediately access additional information or locations that would further enhance their understanding and experience. Instead of just studying about the various systems of the human body, VR applications can be developed to allow them to virtually enter a body and follow the bloodflow through the heart and lungs, or perch themselves inside an ear to watch what happens to the ear drum when sound waves hit it.

Combining tactile and VR communication, it will be possible for students to develop hands-on skills by using simulations of highly sensitive expensive equipment without potentially damaging the real equipment. And medical students can perfect the precise hand motions and pressure required to carry out surgical procedures with applications that even can provide them virtual but realistic feedback on the damage they can do if they do not perform correctly. Students in elementary schools may see the tops of their desks turned into touch-sensitive screens, able to assess their progress as they complete assignments and providing them corrections and directions to increase their success.

One of the populations that has been profoundly impacted by 21st century technology developments are individuals with disabilities. At present, with the model of assistive technology that is device-dependent, where applications have to be within the hardware accessed by the user, many assistive and adaptive technologies are far too costly to be available in schools. However, with 5G and the Cyberverse, where the applications will live in the Cloud and users will access them via a device in their hands or on their wheelchair, expensive speech and language technologies, for example, will be made far more widely available for those children who are unable to speak without such assistance. The impact on the ability of those children to participate in a regular educational setting with their peers will expand exponentially.

Cloud-based robots can be considered as a full-time assistants for students with disabilities, helping them to interact with the standard classroom environment and their peers. Rather than having to call a teacher over for help (which can cost both the student and the teacher time they could be using more productively) the students can take care of the issue with the help of their robot.

At the college level, we look forward to many applications that can improve today's teaching, learning, and campus experience. Being automatically logged into the classroom as soon as entering the classroom, being alerted by a tactile signal as soon as losing concentration during a lecture, or real-time feedback to a lecturer about areas that students still have problem based on the real-time analyses of their notes are all innovations well within reach with 5G and the Cyberverse.

Dakota State University began as a teacher's college, and its education degree programs are still central to its mission. In recent years the university has significantly expanded its

collaborations with K-12 schools in South Dakota, focusing on two needs in cyber education: a general cyber literacy for all students, and accelerated education and opportunities for those who are interested in pursuing cyber careers. These programs will provide a foundation and structure within which SD5G and the SD Cyberverse can begin to develop, test, and implement some of the many exciting teaching/learning innovations that will be enabled by these new technologies.

b) Agriculture

Agriculture is an industry in every state in the union, and in many areas remains a key employer. The United States is a net exporter of food to the world, which has often strengthened both our economic and national security. South Dakota is located in the middle of the country's most agriculturally rich region, and the state's traditional expertise and success in agriculture has continued to move forward. South Dakota is now a leader in technology-based precision agriculture. South Dakota farms are heavily invested in the development and use of automated driving technology, computer vision, telematics, and cloud-based mobile applications to help farmers double or triple their yields -- a feat that will be key to keeping up with global food demands as the Earth's population grows over the next thirty years.

It is a known fact that food sufficiency plays a major role in the peace and prosperity of any country. Predictions are that by 2050 there will be nine billion people on the planet. To feed all those people, experts believe globally agriculture will need to increase current production by 70 percent. It is a race to develop and deploy the technologies to get there, and certainly the first country to do so will reap enormous benefits, not only in its ability to feed its own population but economically to be the preferred marketplace for other countries.

In the early 1800's, it took about 300 hours of labor to produce 100 bushels of wheat. Today in South Dakota, through the application of leading-edge technologies, it takes less than an hour of labor to produce 100 bushels of wheat. However, in the state as around the world, climate change, soil degradation, and water shortages are all challenges that are increasing. Sensors are already available that can be put out in crop fields to collect information such as soil moisture, fertilization, and recent weather impacts. With 5G and the Cyberverse, once the processing is done in the Cloud, these will be able to be simpler and less expensive. The information from the sensors will be able to be transmitted to a central hub, providing farmers real-time access to information and analysis of their land and crop. This information can then be used to logistically plan for the most effective use of their resources like water and machinery.

Cattle farmers in the west to be profitable have to have herds of thousands of animals distributed over thousands of acres of land. The growth, health, and location of those herds is critical information for the rancher. Cattle and sheep often wander into terrain that is inaccessible by motor vehicles, still requiring location and monitoring by horseback, challenging and slow, especially in winter blizzards, when the livestock often need the most support to survive. GPS devices, passive systems requiring only small units with little energy draw, are already available that can be attached to each animal, which would make it possible for real-time monitoring of the location of one animal or a thousand. In addition, biomedical sensors are now available and shrinking in cost and size that will be able to provide real-time biomedical data on livestock, such as body temperature, pulse, growth, and even tissue resistivity, a significant measure of productivity and market value. Today, neither the bandwidth nor the capacity to

accommodate thousands of simultaneous users make this application practical. However, with 5G it will be just one of many that will transform livestock farming.

South Dakota's vigorous agricultural industries, illustrative of agriculture across the United States, are providing expertise and enthusiasm toward the development of 5G and the Cyberverse across the state.

c) Manufacturing

Supplying the needs of the United States through a strong domestic manufacturing sector protects the country from international economic and political disruptions. 5G and the Cyberverse has the responsiveness, concurrency and reach that will transform manufacturing.

One in every ten jobs in South Dakota is in manufacturing. In 2016 the state's manufacturing industry generated more than $4.5 billion of output and accounted for 9% of South Dakota's GDP. The state's manufacturing sector has eagerly sought out technology-based innovations to increase productivity, expand markets, and develop new products. South Dakota's Manufacturing and Technology Solutions (MTS) organization is part of the National Institute of Standards and Technology's Manufacturing Extension Partnership (NIST MEP). MTS is one of many organizations supporting South Dakota manufacturing in its drive for what is being called Industry 4.0, or the next industrial revolution. NIST is advancing 'smart manufacturing' as systems that are "fully-integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs." For example, South Dakota manufacturers are heavily engaged in deploying Collaborative Robots (Cobots) and Autonomous Guided Vehicles (AGVs) on factory floors. South Dakota companies have discovered that implementing these robotic systems improves efficiency, reduces errors, increases safety by relieving humans from dangerous tasks, and reduces machine downtime. Compared to traditional industrial robots, the latest collaborative robots are better suited to high mix, low volume production, meaning they can be used to meet variable demand and for just-in-time inventory processes. However, they also require a more sophisticated technological infrastructure, and large-scale multi-site deployment will require the capabilities of 5G and the Cyberverse.

South Dakota's manufacturing companies will provide the testing ground for how 5G and the Cyberverse need to be configured to support their activities.

d) Health Care

5G and the Cyberverse will have a profound impact on health care delivery in this country, especially for those populations who have historically been underserved. A fast, reliable, high-capacity network will make it possible to truly implement telemedicine, and enable providers, first responders, and even civilians to provide medical aid faster, more efficiently and safely.

The Center for the Advancement of Health Information Technology (CAHIT) is one of the DSU MadLabs and the home of HealthPoint, the non-profit federally-designated health information technology (HIT) resource and support center for all South Dakota healthcare providers. HealthPoint is part of a national network of 60 regional extension centers with a pipeline of key information on health IT. The organization supports medical practices with technology tools and support needed to improve quality of care, increase patients' access to information, utilize health data to determine gaps and

interventions, and spend dollars more wisely. As a result of their work, South Dakota leads the nation in percentage (90.4%) of office-based physicians that have adopted certified Electronic Health Records. SD5G and the SD Cyberverse will use this existing strong network of already-connected medical practices to explore how best to configure the new technologies to enhance and expand medical care delivery.

4) Population clusters and types

South Dakota has a range of population clusters and types and is committed to economic development improvement through the use of technology for all of them. From urban to rural, the state has special focus on making sure the "last mile" and the "last inch" are as connected as the first. South Dakota is also taking the lead in efforts to "revive main street" through migration to 'smart cities,' harnessing the power of technological innovation to improve economic health and the quality of life in our small and medium-sized cities.

South Dakota has the third highest proportion of Native Americans of any state, behind Alaska and New Mexico. Five of the state's counties lie entirely within Indian reservations. South Dakota is also a refugee resettlement state, and its university system has a significant enrollment from international students.

South Dakota is the 11th-fastest growing state in the country, and Sioux Falls is the sixth fastest-growing city in the country. This growth has been significantly fueled by a young (the median age in the state is 36) entrepreneurial culture that is highly tech savvy.

At the same time, the state has a vast land mass and much of the population is distributed in rural areas. In this regard South Dakota is representative of much of the center of the United States, which is often resource-rich but connectivity poor. 5G and the Cyberverse must include innovative ways to connect every U.S. citizen, regardless of their location in the country. SD5G and the SD Cyberverse will develop models to do so.

5) Governmental organizational structures and concerns – city, county, state

The smaller population of South Dakota, and the distributed population, have required that cities, counties, and the state work together collaboratively to meet the needs of the state's citizens. One of the challenges in deploying 5G and the Cyberverse is the complicated, interwoven, and often mutually exclusive regulations, policies, practices, and laws of different municipalities.

One of the greatest needs at the federal level is for new radio spectrum bands to be made available for 5G and the Cyberverse. Senator Thune took the lead toward action on this almost two years ago in the Mobile Now Act proposing reforms that would ensure more spectrum is made available for commercial use and by reducing the red tape associated with building wireless networks. His leadership and interest in moving U.S. technology and networking forward is matched by leadership across South Dakota, and thus the state is a receptive area for developing, deploying, and creating best practices for leading edge technologies.

6) Geographies and climates

The United States is a country which, because of its size, has a vast assortment of geographic configurations and climates. A range of 5G and Cyberverse hardware must be developed and deployed that can accommodate the differences in geographic configurations (e.g., mountains) and extremes of temperature (e.g., hot summers and sub-zero winters), wind, and precipitation. Because of its considerable size – the state is 380 miles long and 210 miles wide – it covers several geographic areas, each with a different weather pattern. The eastern half of the state has a humid continental climate while the western half of the state falls into the semiarid steppe

category. South Dakotans face extremes in temperature: blazing heat waves in the summer and bitter Arctic incursions in winter. In July and August, the mercury can soar above 100 degrees Fahrenheit, while in winter, it regularly dips below zero. Record-setting temperatures in the state include readings above 115 degrees and colder than minus 40. This makes it an ideal setting to test the weatherability of various technologies, and most especially the ability to maintain the network of connectivity under extreme conditions.

CONCLUSION

It is exceedingly important to do what we can to remove the existing barriers to broadband deployment on the horizon of next generation wireless technology deployment, to encourage investment in next generation communications services, and find ways to streamline broadband deployment siting.

I believe the best way to address all three of these issues will start with a coordinated effort to develop widespread understanding and knowledge of what 5G and the Cyber Universe are and why it is so important to the economic, security, and quality of life health for the United States in both the near and far future. To develop and deploy these new technologies in a manner consistent with the country's democratic values and concerns, we must engage cyber security professionals in every aspect of this testbed. I believe the way to make the greatest progress most rapidly is to create a public/private partnership to build and deploy a real-world 5G and Cyberverse testbed. We are eager to do so in South Dakota, as a geographic area in the U.S. that contains a cross-section of the types of population clusters and organizations, geography, climate, industries, and existing technologies, to explore, troubleshoot, and establish best-practice models for the technology as well as the policies and governance required to support 5G development and deployment across the country.

5G and the new Cyberverse is a common good whose availability and operability will be critical to every endeavor across the United States. As such, it is important that the federal government provide leadership and support for those efforts that will move development and deployment of this vital national resource.

It is also the case that we will only get one chance to do this first. The United States was the first country to develop and implement the comprehensive Internet, initially building on the foundation and integrating multiple federally-developed networks. The results have been clear and impressive. Despite all of the concerns about cyber security issues and technology dependencies, there is no question that the United States lead in developing and deploying the Internet has had profound economic and societal impacts. There is a need once again for the federal government to step forward and take the lead in investment and organizational support for the development and deployment of 5G and the Cyberverse.