



Intro

As the Department of Homeland Security has pointed out in various critical infrastructure assessments, mobile networks are no longer dedicated to telephony, Internet access and video streaming. Today's mobile network is an essential foundation of public safety, industrial productivity and national security, on equal footing with other components making up the communications sector. The deployment of 5G networks will significantly increase the value and importance of mobile networks to national security, economic competitiveness, and public health and safety.

Arm provides the computing architecture and microprocessor designs for billions of devices worldwide. Arm's chip designs can be found from the smallest, most energy efficient designs in internet of things (IoT) devices to the most powerful supercomputer in the world¹, and all forms of computing in between. This includes mobile networks, where Arm-based processors are nearly ubiquitous in radio access network (RAN) equipment. As such, Arm has a vested interest in ensuring 5G is deployed rapidly and securely and is pleased to have the opportunity to provide these comments to inform NTIA's decision-making on 5G related matters.

Line of Effort One: Facilitate Domestic 5G Rollout.

The U.S. Federal Government should significantly increase its investment of research and development related to the key technologies that underpin mobile networks and incentivize companies to invest more into R&D. Semiconductor technology is foundational to 5G development and should be prioritized. As a company, Arm regularly reinvests more than 30% of its revenue back into research and development, and the semiconductor industry at large outpaces nearly every other industry in R&D reinvestment percentage. As the global economy tightens as it appears to be doing, these reinvestments become more difficult to make however without government support and incentives. The Semiconductor Industry Association has quantified the return on investment achieved through federal semiconductor R&D spending.² Further, Congress has recognized the need to further invest in, and incentivize private sector spending on semiconductors and related technology with the introduction of the Creating Helpful Incentives to Produce Semiconductors for America Act or "CHIPS" Act.³

¹ See *Japan's Arm-powered Fugaku named world's fastest supercomputer*, <https://www.datacenterdynamics.com/en/news/japans-arm-powered-fugaku-named-worlds-fastest-supercomputer/>

² See *Sparking Innovation: How Federal Investment in Semiconductor R&D Spurs U.S. Economic Growth and Job Creation*, <https://www.semiconductors.org/sparking-innovation/>

³ Legislation introduced as S. 3933 in the U.S. Senate, and as H.R. 7178 in the U.S. House of Representatives; "5G leadership" being cited by the bills' sponsors and cosponsors as an aim of the bill. See <https://www.cornyn.senate.gov/node/5599>



The U.S. should also prioritize making additional spectrum, in particular mid- and lower-frequency spectrum available for mobile networks. This spectrum will be essential in providing broader coverage that cannot be achieved with higher frequency, particularly millimeter-wave spectrum. While a mix of low-, mid-, and high- frequency spectrum will be essential for 5G, the U.S. should prioritize working with incumbent users of sub-6GHz spectrum to ensure the U.S. keeps up with other countries making spectrum available in those frequencies for 5G service.

The U.S. also needs to streamline broadband infrastructure siting processes. With a more robust network and need to place more equipment in closer proximity for 5G networks, broadband equipment citing issues that have frustrated deployments of previous generations of mobile technology will be exacerbated as 5G is rolled out. This is an issue that must be prioritized at the Federal level by Congress and the Administration to ensure 5G networks can be more efficiently and rapidly deployed without unnecessary delays.

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure.

The U.S. has a number of existing entities and approaches to assess and manage security risks of 5G infrastructure. In particular, the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security has expertise and existing relationships with industry stakeholder to coordinate security across the communications sector. Updates to guidance documents, such as CISA's National Infrastructure Protection Plan, and the Communications' Sector Specific Plan can address new and changing security challenges while building on the key principles and well-defined roles of all stakeholders from the public and private sectors.

The March 2019 Prague 5G Security Conference Principles also provide a thorough collection of principles and policy, technology and security proposals to address 5G security.⁴ Further, it has resulted in a working group of countries the U.S. can coordinate and work with to ensure common approach to 5G security are established and leveraged among like-minded allies.

Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

It is hard to predict the type or extent of economic impacts the deployment of 5G will bring. The emergence and growth of the app and sharing economy from 4G was unexpected and unprecedented. The 5G era, however, has the potential to create even more innovation and economic growth due to the significant differences in the network itself. Whereas 4G and all the predecessor wireless technologies were developed for the number of mobile and smart phones that would be connected to the network, 5G is being developed and architected to

⁴ See <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>



connect an exponentially larger number of “things”. This will allow entire industries to be connected and automated, creating opportunity to drive efficiency in processes and work environments never before thought possible.

The maturation of 5G alone is not driving this, but also IoT and advancements in machine learning and artificial intelligence. The combination of these will allow connected computing to happen in more places, bringing new efficiencies and innovations to more sectors. Economic opportunities will likely come in three areas:

- 1) diversity of network supply chain – the US and others are looking at alternative mobile network architectures that could change the mobile network equipment market to be more open and interoperable. This could create opportunities for US companies to be more competitive in supplying mobile network hardware and software.
- 2) new and fully realized uses – as 4G brought wider utilization and growth of social media, and spawned creation of platforms like ride sharing, 5G will almost certainly create new, yet to be conceived of companies and markets.
- 3) automation - through a combination of the ability to easily connect machines over 5G networks, as well as other advances in technology, manufacturing and other production capabilities will be able to more easily be automated. This could alter incentives for certain manufacturing to be done overseas due to labor costs, safety concerns, or other human factors, and result in increased production in the U.S.

To the questions of vendor diversity, 5G brings the prospect of wider use of ‘virtualization’, that is using software-based networks. This introduces the possibility of a RAN operating through software sitting on top of basic core equipment. There is very interesting and promising work occurring around this in bodies like 3GPP, O-RAN Alliance, and the Telecom Infra Project. The government should support these efforts, while also recognizing the important role traditional mobile network equipment companies will play in 5G deployment. To do this, it is important to enact policies that promote innovation and experimentation, but do not mandate specific technologies. For example, the government should:

- ensure all technologies can be used in 5G networks but don’t mandate specific technologies; remain technology agnostic in supporting 5G deployments
- utilize government procurement as a means to support vendor diversity
- create demo deployments with new technologies on govt facilities like military bases⁵
- ensure government funding supporting 5G deployments (USF, RUS, etc) can utilize all technologies, including new and competitive technologies

⁵ For example, projects like this could serve as testbeds:

<https://www.defense.gov/Newsroom/Releases/Release/Article/2206761/dod-names-seven-installations-as-sites-for-second-round-of-5g-technology-testin/>



There will be a key role for the government to play in workforce development and upskilling if there are changes to the single vendor network deployment model that is prevalent today. Today, typically one company provides the RAN equipment, as well as installing, maintaining, upgrading, and providing all other services necessary to keep it working properly. If the model and multiple vendors are providing software and hardware components into a mobile network, that ability to install and maintain it becomes more complicated. It may require a third party or the MNO to train workers to manage that. The government could facilitate this by starting to look at training requirements, support training programs, or providing other support for these new skills and needs in the workforce.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

The US Government should use all tools and mechanisms it has to partner in a collaborative way with allies and like-minded countries to promote the development and deployment of secure 5G technology. All bilateral, multilateral and plurilateral engagements should address this, including prioritizing 5G cooperation in science and technology agreements and free trade agreements. Similar to how cybersecurity cooperation has been prioritized through these mechanisms in the past, 5G should be similarly prioritized.

Further, the government must ensure U.S. companies and entities are able to fully participate in standards setting bodies and activities contributing to 5G standards development. Entity listings and other government action which create confusion about the ability of U.S. citizens and companies to participate in this activity, or worse strictly prohibits them from doing so, puts the U.S. at a disadvantage in contributing to the development of these standards. The clarification from the Department of Commerce on the ability of U.S. companies and individuals to participate in some standards activity that had been in question following the inclusion of Huawei and affiliated companies on the denied entity list was a positive step in addressing this.⁶

Respectfully Submitted,
Vince Jesaitis
Director, Government Affairs
Arm, Inc.

25 June 2020

⁶ See <https://www.commerce.gov/news/press-releases/2020/06/commerce-clears-way-us-companies-more-fully-engage-tech-standards>