PREPARED STATEMENT FOR THE RECORD OF

INTEL CORPORATION

For the

UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORATION

Hearing On

5G SUPPPLY CHAIN SECURITY: THREATS AND SOLUTIONS

MARCH 4, 2020

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for inviting Intel to speak about 5G supply chain security. I serve as Corporate Vice President in engineering, responsible for next generation technology and standards at Intel Corporation. In this role, I am responsible for future products including the convergence of communications, compute and artificial intelligence and defining the future networks towards 6G. My responsibilities also include Intel's contributions to industry standards and the company's leadership in global forums including IEEE, 3GPP and multiple industry fora. It is my job to drive the benefits of 5G to various other businesses by fueling innovation for homes, cities and enterprise.

Intel Corporation is a U.S. semiconductor manufacturer headquartered in Santa Clara, California that employs over 100,000 people globally, with more than half of those in the United States. Intel is the largest global semiconductor supplier, with the majority of our advanced manufacturing and research and development (R&D) is conducted in the United States. Revenue earned in global markets contributes to Intel's Annual R&D and Capital Investments of 29.6 billion dollars.[1] Intel is one of the last integrated device manufacturers (IDM) in the United States. This means Intel owns production for most of its products from conception, through design, to manufacturing, all the way to delivery to a device manufacturer. Having most of our design and fabrication within the same company creates significant technology advantages for Intel in setting the highest standards for quality, consistency and security. And when we identify problems, the IDM model creates advantages for Intel in resolving problems rapidly.

Intel's processors, memory, storage and other products power much of the world's computing capability. Intel is a leader in 5G and one of our roles is to supply high volume and high-quality products to telecom equipment manufacturers. By 2021, we are expected to become the world's largest silicon provider for 5G infrastructure. 5G runs on Intel. It used to be Intel inside computers and data centers, but now Intel is inside the network as well.

[1] [1] Source: 2019 Q4 10K filing from Intel Corporation, https://www.intc.com/investor-relations/financials-and-filings/earnings-results/default.aspx

Intel also participates in over 250 standards and industry groups worldwide including industry alliances, regional standards organizations, international industry standards groups and formal international standards bodies. For 5G standards involvement, Intel holds leadership positions in 3GPP, IEEE, and the International Telecommunications Union. Intel is also a board member of the Telecom Infra Project and a member of the ORAN Alliance. Intel also participates in the new ATIS 5G Supply Chain Working Group tasked by the Department of Defense with developing standards and evaluating certification options necessary to establish "assured" commercial 5G networks.

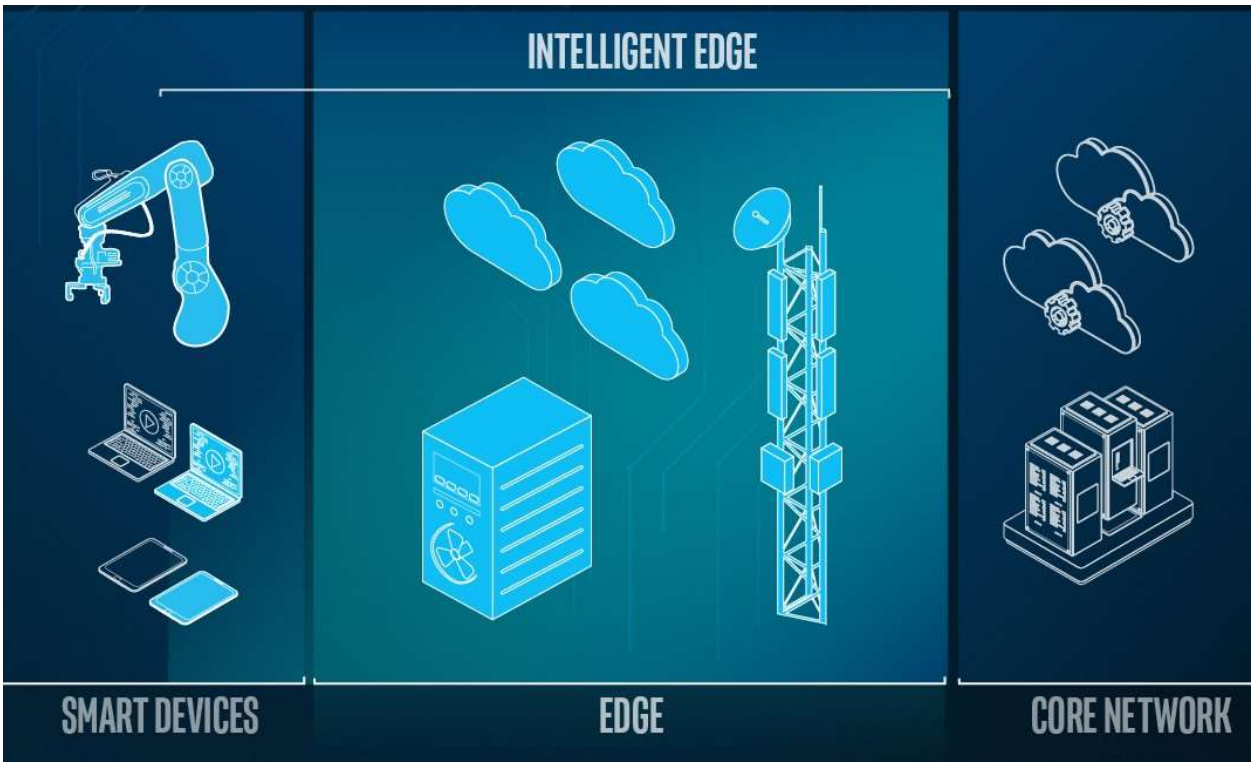
For today's discussion on 5G supply chains, I would like to begin by discussing some developments regarding 5G networks followed by some important considerations regarding supply chains.

5G networks:

5G marks the convergence of communications and compute capabilities, a world in which 5G, Wi-Fi, artificial intelligence, the cloud, and edge computing combine to fundamentally change our world. The U.S. was the first nation with widespread 4G coverage which led to many innovations that many of us use every day on our smartphones from ordering rides to groceries to take-out dinners to checking in for flights to reading books or watching shows. 5G will enable these types of benefits to businesses in many different industries such industrial IoT in manufacturing, mining, agriculture, healthcare, etc.

Virtualization is critical to enable to transition to 5G. Radio Access Network (RAN) architectures are evolving to support a diverse set of deployments. As part of this evolution, some of the network functions are virtualized rather than being served by discrete products, creating what are called virtual Radio Access Networks. An analogy would be if you previously needed one computer to do presentations, another computer to browse the internet, another computer for email, etc. but now you can do all those functions on a single computer. This way you can use the processing power on the application that needs it the most at a specific point in time.

Network virtualization has been a ten-year journey across the communications industry, which started at the core of the network to service provider metro and neighborhood central offices - and now out to the RAN, the last link between users and the network (e.g. cell tower to end user). Network virtualization enables the agility of software-based innovation. Just as this approach enabled the dot com companies of the 90s to provide new services to consumers, software innovation including Virtual RANs are intended to enable a breadth of service opportunity in telecommunications.



3GPP is developing a global 5G standard which will be implemented in networks worldwide. These networks will include traditional cellular operators as well as new entrants. Different services providers will take steps in network virtualization on varying timelines, so different options will exist ranging from the traditional telecommunications equipment manufacturer model to the different flavors of Virtual RAN. Open RAN, such as the work within the Open RAN Alliance, is one version of a Virtual RAN. The Open RAN Alliance is working to develop an interoperable specification with open interfaces between the base stations and the radio which enables cellular operators to utilize different vendors.

Intel's product lines support the various approaches ranging from traditional telecom equipment manufacturers (e.g. Ericsson and Nokia), so they can continue to deliver products to ensure continuity in telecom industry, to new entrants (e.g. Altiostar and Mavenir) through our rich software development kit, open source activities and reference platform designs.

Technology Supply Chains

We recognize there are security challenges to overcome. Worldwide, policymakers have begun to focus on supply chain risks in new ways. In August 2018, MITRE published the highly influential report, Deliver Uncompromised, which described the urgency and importance for supply chain risks to receive attention during product procurement. New U.S. laws, including the 2018 SECURE Technology Act, gave federal agencies new authority to consider supply chain risks when procuring products. From Europe's "digital sovereignty" efforts to Japan's "Cyber/Physical Security Framework" efforts, there are signs of strong interest in shining a

spotlight on the trust and transparency of supply chains for information and communications technology.

Intel will continue our proactive efforts to build a more trusted foundation for all computing systems. Intel's unique position in the technology supply chain has allowed us to take a leading role, in partnership with our suppliers and customers, when it comes to transparency and security. Intel's supply chain depends on successful, consistent, and trustworthy relationships with roughly 14,000 companies who provide Intel with the raw materials, products and services required for us to supply technology to over 2,100 customers. The collaboration and commitment occur across the supply chain – from Intel's suppliers, through Intel internal production, and outbound to Intel's customers.

Intel identifies four key stages in the compute supply chain: build, transfer, operate and retire. Each stage includes unique threats. Examples of these threats include:

Build

- Injection of malicious code, logic or components during design or manufacturing
- Cyber-attack against a supplier resulting in denial of service (DOS), supply chain disruption, data corruption, data breach

Transfer

- Counterfeit for profit, sabotage, or other reason
- Interdiction and tampering during manufacturing or transit

Operate

- Compromising administrator credentials
- Installation of vulnerable code or components

Retire

- Theft of components / data from retired system
- Appropriate of residual data left on systems

Compute Lifecycle Assurance

Addressing the gap between trustworthiness and 'leap of faith' is a primary motivation for a new Intel initiative designed to help increase data available to end user customers about the supply chain that brings computing devices to your doorstep. Intel describes the effort as "Compute Lifecycle Assurance," and it starts with the goal of making supply chains more transparent.

Intel has tackled big, complex problems like this before. We actively led and collaborated with the industry to influence policies and processes concerning the use of conflict-free minerals — not only for Intel products — but across the industry. In addition, we have already developed a set of policies and procedures at our own factories to validate where and when every component of a server was manufactured. These examples represent an important beginning, and there is more that can be done.

In today's increasingly complex supply chain environment, we want to provide our customers with a full range of tools and solutions that deliver assurances of integrity throughout the entire lifetime of a platform. This starts with a security-first approach to design. It continues as platforms change custody, ownership and physical location several times during their assembly, transportation and provisioning. Once operational, they may then require updates for optimal performance and security. Finally, upon retirement from service, platforms should ensure the confidentiality of data that was transmitted, erased or stored.

The industry needs an end-to-end framework that can be applied across this multiyear life of any platform. And that is our goal with the Compute Lifecycle Assurance Initiative — to substantially improve transparency and to provide higher levels of assurance that improve integrity, resilience and security during the entire platform lifecycle.

Today Intel is working to:

- Invest in tools and processes that improve the integrity of Intel computing products across every lifecycle stage, building on the Transparent Supply Chain tools we have today.
- Contribute best practices, learned from our decades of experience, for the collection, measurement, stewardship and reporting of platform data to meet our customers' evolving needs.
- Collaborate with the ecosystem to develop innovative ways that enhance access to platform data while maintaining confidentiality of that data across the platform lifecycle.

Policy Considerations

The United States government has a valuable role to play in the 5G supply chain by encouraging and supporting the emergence of a vibrant and trusted ecosystem. Intel commends the work done in 2019 by the Department of Homeland Security's Supply Chain Risk Management task force and sees this type of public sector-industry collaboration as vital to identifying and solving important questions about technology supply chain. Likewise, the work done by the Commerce Department's National Institute of Standards and Technology (NIST), has been extremely helpful in creating common goals and frameworks for progress among policymakers and industry. Intel has been active in these and other efforts to offer its expertise and insight in addressing supply chain risks and mitigations.

Given the potential of 5G to provide valuable benefits to American businesses and consumers, the United States government should take measures to help facilitate widespread 5G deployments. Intel has advocated extensively for mid-band spectrum. Mechanisms to encourage increased investments in 5G infrastructure and to facilitate continued innovation throughout the 5G ecosystem will be critical. We appreciate Congressional and Executive Branch interest in areas such as potential broadband infrastructure deployment funding,), and ways to spur innovation and deployments in 5G such as the USA Telecoms Act, which serves as a good starting point for further discussion.