

December 4, 2019



Intel Editorial: Advancing Industrywide Compute Lifecycle Assurance

Assurance Begins with Security-First Design and Extends Throughout the Compute Lifecycle

SANTA CLARA, Calif.--(BUSINESS WIRE)-- The following is an opinion editorial from Leslie Culbertson of Intel Corporation.

This press release features multimedia. View the full release here:

<https://www.businesswire.com/news/home/20191204005239/en/>

Leslie S. Culbertson is an executive vice president and general manager of Product Assurance and Security at Intel Corporation. (Credit: Intel Corporation)

The globalization of technology design, development, manufacturing and distribution has created an environment of complicated supply chains with limited transparency.

There is a growing need to provide assurances of platform integrity in every stage of the compute lifecycle, and to do so in a manner that is as transparent as possible. Government agencies, commercial organizations and consumers deserve this transparency and the benefit it can bring for improved platform security and resiliency.

This presents both an incredible challenge and opportunity for the ecosystem. Today, Intel is responding to the challenge with the introduction of our Compute Lifecycle Assurance Initiative.

We have tackled big, complex problems like this before and we are doing it again. Intel has already taken several important steps toward supply chain transparency. 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 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.

More: [Introduction to Compute Lifecycle Assurance](#) | [Security News at Intel](#)

We have identified four key lifecycle stages: build, transfer, operate and retire. Over the next year, we commit 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.

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](#). MITRE's report 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 U.S. 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.

We believe a broader set of commercial enterprises from around the world will find value in this level of assurance for validation, compliance and governance. In the next 12 to 18 months, we expect to see growing interest from our customers, partners and government oversight organizations to improve transparency beyond the manufacturing supply chain to also include transportation, provisioning, attestation and in-field updates.

We're in a unique and fortunate position as a trusted member of the ecosystem and as a leader in the transparency of our own supply chain. We intend to use this position to help mobilize the industry at large and to anticipate the needs of our global — and mutual — customers.

These are early days, and we know we can't do this alone. We invite the broader ecosystem to join us on this journey. Together with our partners and customers, we will continue to build a more trusted foundation for all computing systems.

[Leslie S. Culbertson](#) is an executive vice president and general manager of Product Assurance and Security at Intel Corporation.

About Intel

Intel (NASDAQ: INTC), a leader in the semiconductor industry, is shaping the data-centric future with computing and communications technology that is the foundation of the world's innovations. The company's engineering expertise is helping address the world's greatest

challenges as well as helping secure, power and connect billions of devices and the infrastructure of the smart, connected world – from the cloud to the network to the edge and everything in between. Find more information about Intel at newsroom.intel.com and intel.com.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

View source version on businesswire.com:

<https://www.businesswire.com/news/home/20191204005239/en/>

Leigh Rosenwald

503-784-7492

leigh.rosenwald@intel.com

Source: Intel Corporation