Forward-Looking Statements

Statements in this press release that refer to future plans and expectations, including with respect to Intel’s manufacturing expansion and investment plans in the European Union (EU), are forward-looking statements that involve a number of risks and uncertainties. Words such as “anticipates,” “expects,” “intends,” “goals,” “plans,” “believes,” “seeks,” “estimates,” “continues,” “may,” “will,” “would,” “on track,” “should,” “could,” and variations of such words and similar expressions are intended to identify such forward-looking statements. Statements that refer to or are based on estimates, forecasts, projections, uncertain events or assumptions, including statements relating to the anticipated benefits of Intel’s planned EU investments, including with respect to meeting future demand and future capacity expansion; anticipated supplier, ecosystem, community, and government support and approval for Intel’s planned EU investments and anticipated benefits related to such support; the proposed transaction between Intel and Tower Semiconductor (Tower), including statements regarding the benefits and the timing of the transaction, as well as statements regarding the companies’ products, customers, and markets; additional future site investments and the timing of such investments; anticipated construction and production timing for Intel’s planned factories; future products and technology and the availability and benefits of such products and technology, including future transistor technology; environmental plans for and benefits from Intel’s factories and technologies, including regarding energy use, water use, and waste; future external foundry business; plans and goals related to Intel’s foundry business; foundry service offerings; market opportunity; and anticipated trends in our businesses or the markets relevant to them, also identify forward-looking statements. Such statements are based on management’s expectations as of the date they were first made and involve risks and uncertainties that could cause our actual results to differ materially from those expressed or implied in our forward-looking statements. Important factors that could cause actual results to differ materially include, among others, Intel’s failure to realize the anticipated benefits of its strategy, plans, and proposed transactions; construction delays or changes in plans due to business, economic, or other factors; increases in capital requirements and changes in capital investment plans; adverse changes in anticipated government incentives and associated approval related to Intel’s planned EU investments; adverse legislative or other government actions; insufficient ecosystem support; the risk that the proposed transaction with Tower may not be completed in a timely manner or at all; uncertainties as to the timing of the consummation of the Tower transaction and the potential failure to satisfy the conditions to the consummation of the transaction, including the receipt of certain governmental and regulatory approvals; demands in Tower customer end markets and for Tower foundry services and/or products that exceed Tower’s capacity; the impact of macroeconomic and geopolitical trends and events; and the factors set forth in Intel’s Securities and Exchange Commission (SEC) filings, including the company’s most recent reports on Forms 10-K and 10-Q, which may be obtained by visiting our Investor Relations website at www.intc.com or the SEC’s website at www.sec.gov. Intel does not undertake, and expressly disclaims any duty, to update any statement made in this press release, whether as a result of new information, new developments or otherwise, except to the extent that disclosure may be required by law.
Greg Lavender
SVP, CTO and GM of Intel’s Software and Advanced Technology Group
Rapid Digital Transformation
Creates an ever-increasing attack surface
New ransomware attack
every 2 seconds
by 2031

Source: Cybersecurity Ventures
Design and engineer with a Security-First Mindset
Delivering Security Technologies for Today and Tomorrow

- Confidential Computing
- Secure & Responsible AI
- Preparing for the Era of Quantum Computing
The trusted choice for delivering a Secure Computing Environment
Intel Threat Detection Technology (TDT)
Identifying malware and improving endpoint detection and response

Hardware-enforced Security Providing a Root of Trust

Intel Control-flow Enforcement Technology
Designed to protect businesses against common malware attacks
Encryption technologies that enable Protection of Data
Confidential Computing

Protecting Data-in-use Cloud to Edge

**Trusted Execution Environment (TEE)**
Hardware-enforced separation between data processing and the platform owner

**Intel Software Guard Extensions (SGX)**
Confidential computing in a virtualized environment through application isolation
Trusted Execution Environment

Intel Software Guard Extension (SGX)

Intel Trust Domain Extensions (TDX)

Confidential Computing beyond the CPU

Today

In the near future
Trustworthiness of the confidential compute environment
Extending Attestation Services in cloud environments

Project Amber
Intel’s Trust-as-a-Service
Software-first Strategy
Competitive advantage that offers new value realization avenues for our ecosystem partners and customers

- Market-Making Technologies
- Market-Differentiating Software
- Market-Enabling Technologies
Easy Deployment of Confidential Computing Solutions using Intel SGX without application code modification
Scaling Technology up the Stack by leveraging Intel’s software and hardware technologies
AI and Machine Learning
Responsible deployment across verticals
Pushing the Boundaries for securing AI models and protecting the privacy of data
Securing AI Models

Intel OpenVINO machine learning platform
Intel-led open-source Gramine project
Intel Software Guard Extensions
Commitment to Responsible AI
Secure data access for healthcare
Intel Software Guard Extensions

30-40% greater acceleration of medical AI innovation

Intel Software Guard Extensions

Microsoft Azure’s Confidential Computing

For workloads and configurations visit www.Intel.com/PerformanceIndex. Click on the Events tab and Vision Event Claims. Results may vary.
Open Federated Learning

55 enabled medical institutions across six continents
Intel Software Guard Extensions

33% improved efforts to locate tumors

Securing AI models

For workloads and configurations visit www.Intel.com/PerformanceIndex. Click on the Events tab and Vision Event Claims. Results may vary.
FakeCatcher
World’s first real-time deepfake detection platform
Quantum Computers will provide computational power, far exceeding traditional computers. And will weaken and ultimately break cryptography.
Preparing for the Era of Quantum Computing

Leading the industry with quantum resistant innovations

The time to act is now

Quantum-Resistant by 2030
Post Quantum Crypto
Standardization Efforts

Built-in Crypto Acceleration
algorithmic and software innovations for breakthrough performance

New Class of Quantum-resistant Crypto
for next-generation security without sacrificing performance

Today

2030
Internet Engineering Task Force (IETF)
National Institute of Standards and Technology (NIST)
International Organization for Standardization (ISO)

Post Quantum Crypto Standardization Efforts
Preparing for the Era of Quantum Computing

Quantum-Resistant by 2030

Developing Building Blocks for Post Quantum Crypto
three-phased approach

- Increase key sizes by replacing AES-128 algorithm with AES-256
- Increasing the robustness of code with quantum algorithms
- Replacing public key algorithms with post-quantum crypto algorithms
Preparing for the Era of Quantum Computing

Together we can deliver Quantum-Crypto

Quantum-Resistant by 2030
Thank you
Legal Notices and Disclaimers

For notices, disclaimers, and details about performance claims, visit www.intel.com/PerformanceIndex or scan the QR code:

From the landing page, go to the Events tab and then to Vision Event Claims.

© 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.