Breaking the Intel Code

Key Contributors: Jon Chapa
Andrew Deno
Osvaldo Garza

9/30/22

This project and the preparation of this report were funded in part by ….through an agreement with the University of the Incarnate Word.
Cyber Security Systems and the University of the Incarnate Word

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In this report we researched the Intel corporation policies, procedures, protocols, and tools used to protect the sensitive information of users. Our report includes policies ranging from automotive, the environment, human rights, international trade, and lastly cybersecurity. Intel uses industry collaboration, co-engineering, IoT devices, and open source collaborations in order to create innovative software that improves the life of every person on the planet.

Project Milestones:

1. Background of the Intel Corporation
2. Management Overview
3. Policies that the Intel Corporation adheres to and enforces
4. Cybersecurity Foundation

Materials List:

1. Gantt Chart
2. Trello
3. GitHub

Deliverables: E.g. Report, Deployed architecture, other project outcomes, etc.

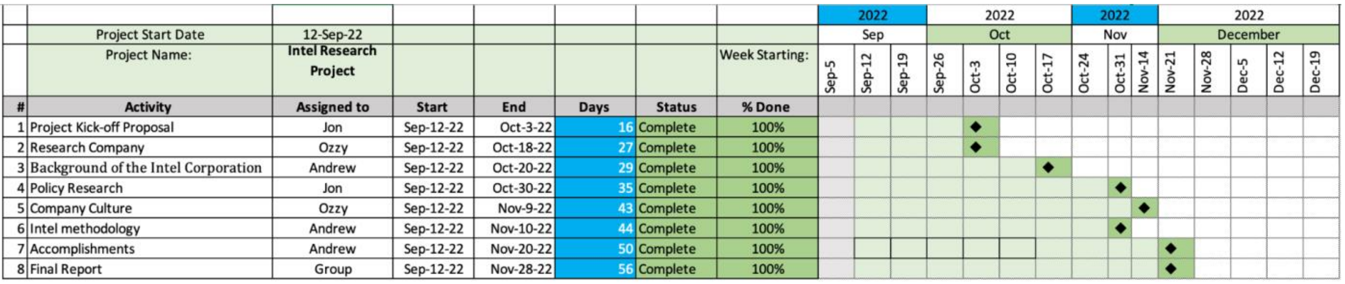
1. Synthesis and analysis from research
2. Understanding of the Intel methodology
3. Explain the policies Intel enforces

Professional Accomplishments: E.g. New skills that you developed

1. Critical Thinking
2. Collaboration
3. Problem Solving

PROJECT SCHEDULE MANAGEMENT

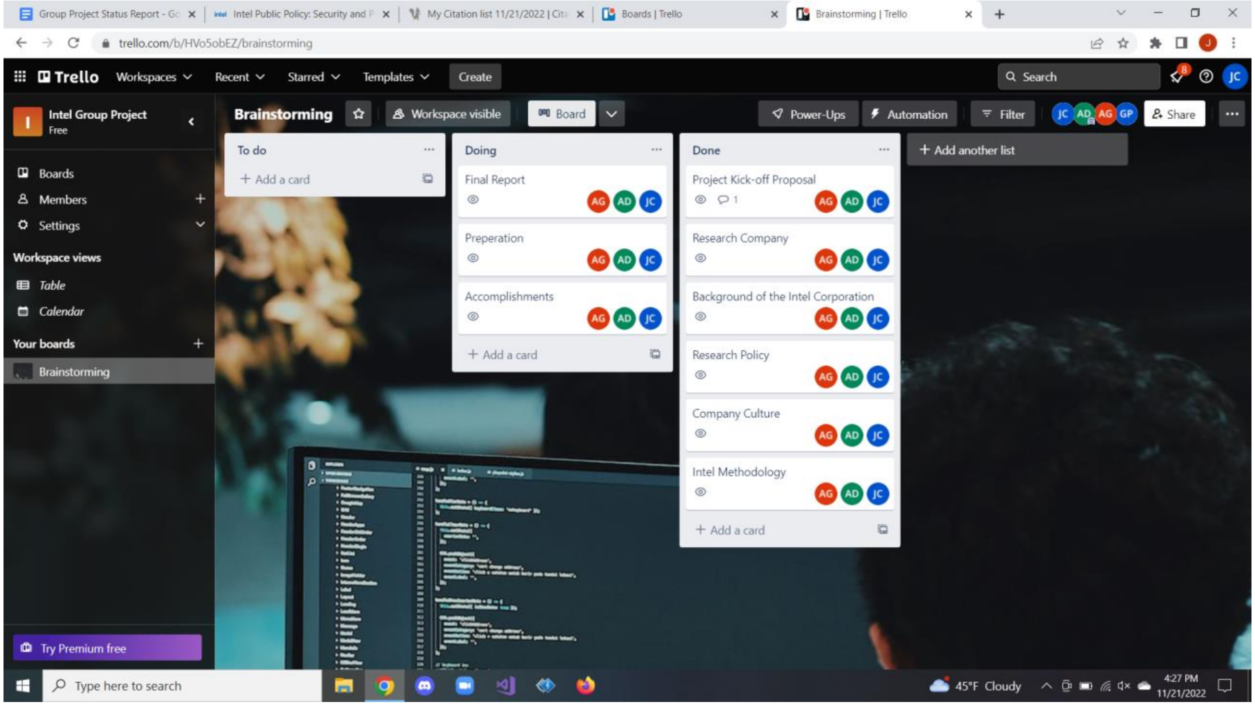
Gantt chart



								2022			2022				2022			2022				
	Project Start Date	12-Sep-22						Sep			Oct				Nov			December				
	Project Name:	Intel Research Project					Week Starting:	Sep-5	Sep-12	Sep-19	Sep-26	Oct-3	Oct-10	Oct-17	Oct-24	Oct-31	Nov-14	Nov-21	Nov-28	Dec-5	Dec-12	Dec-19
#	Activity	Assigned to	Start	End	Days	Status	% Done															
1	Project Kick-off Proposal	Jon	Sep-12-22	Oct-3-22	16	Complete	100%					◆										
2	Research Company	Ozzy	Sep-12-22	Oct-18-22	27	Complete	100%					◆										
3	Background of the Intel Corporation	Andrew	Sep-12-22	Oct-20-22	29	Complete	100%							◆								
4	Policy Research	Jon	Sep-12-22	Oct-30-22	35	Complete	100%									◆						
5	Company Culture	Ozzy	Sep-12-22	Nov-9-22	43	Complete	100%										◆					
6	Intel methodology	Andrew	Sep-12-22	Nov-10-22	44	Complete	100%									◆						
7	Accomplishments	Andrew	Sep-12-22	Nov-20-22	50	Complete	100%											◆				
8	Final Report	Group	Sep-12-22	Nov-28-22	56	Complete	100%											◆				

Statuses
Not started
In Progress
Blocked
Complete

Trello



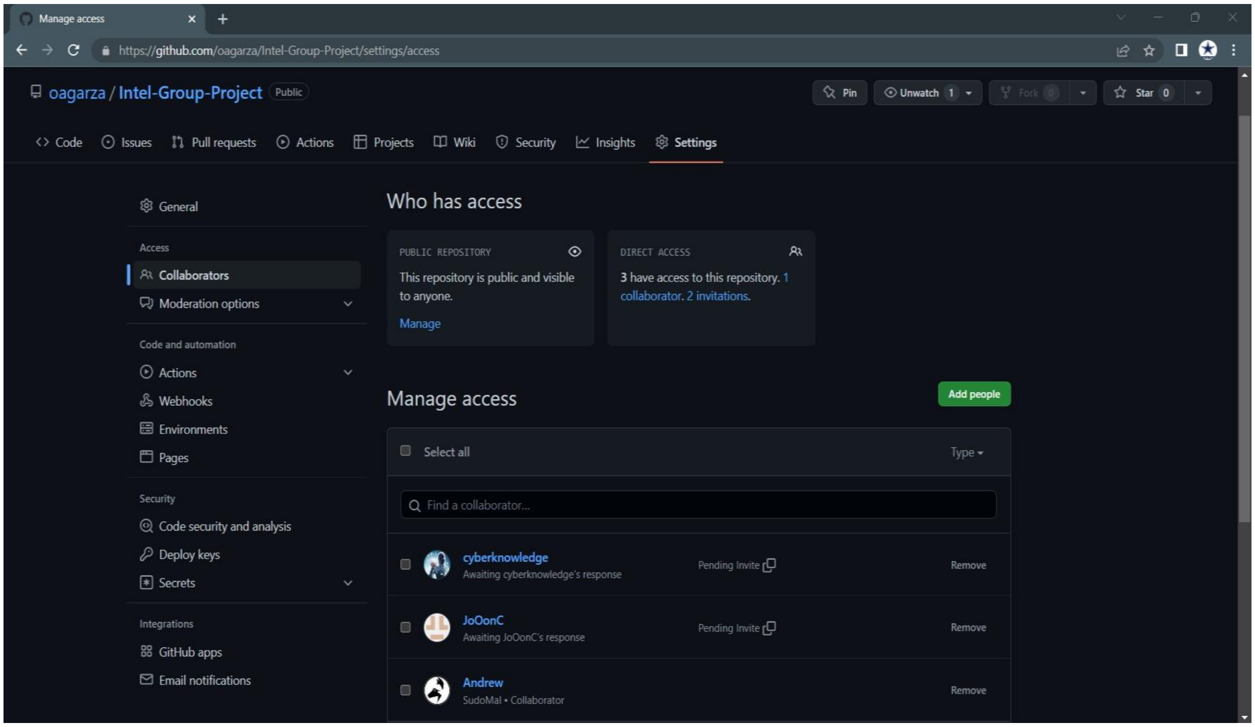
To do
+ Add a card

Doing
Final Report — AG AD JC
Preperation — AG AD JC
Accomplishments — AG AD JC
+ Add a card

Done
Project Kick-off Proposal — 1 — AG AD JC
Research Company — AG AD JC
Background of the Intel Corporation — AG AD JC
Research Policy — AG AD JC
Company Culture — AG AD JC
Intel Methodology — AG AD JC
+ Add a card

+ Add another list

Project Management Board Link (QR Code Only). Send invite to user: @gdparra



Who has access

PUBLIC REPOSITORY

This repository is public and visible to anyone.

Manage

DIRECT ACCESS

3 have access to this repository. 1 collaborator. 2 invitations.

Manage access

cyberknowledge Awaiting cyberknowledge's response	Pending Invite
JoOonC Awaiting JoOonC's response	Pending Invite
Andrew SudoMal • Collaborator	

Create a Github Project Repository and add the user “cyberknowledge” as a contributor.

https://github.com/oagarza/Intel-Group-Project

RESEARCH

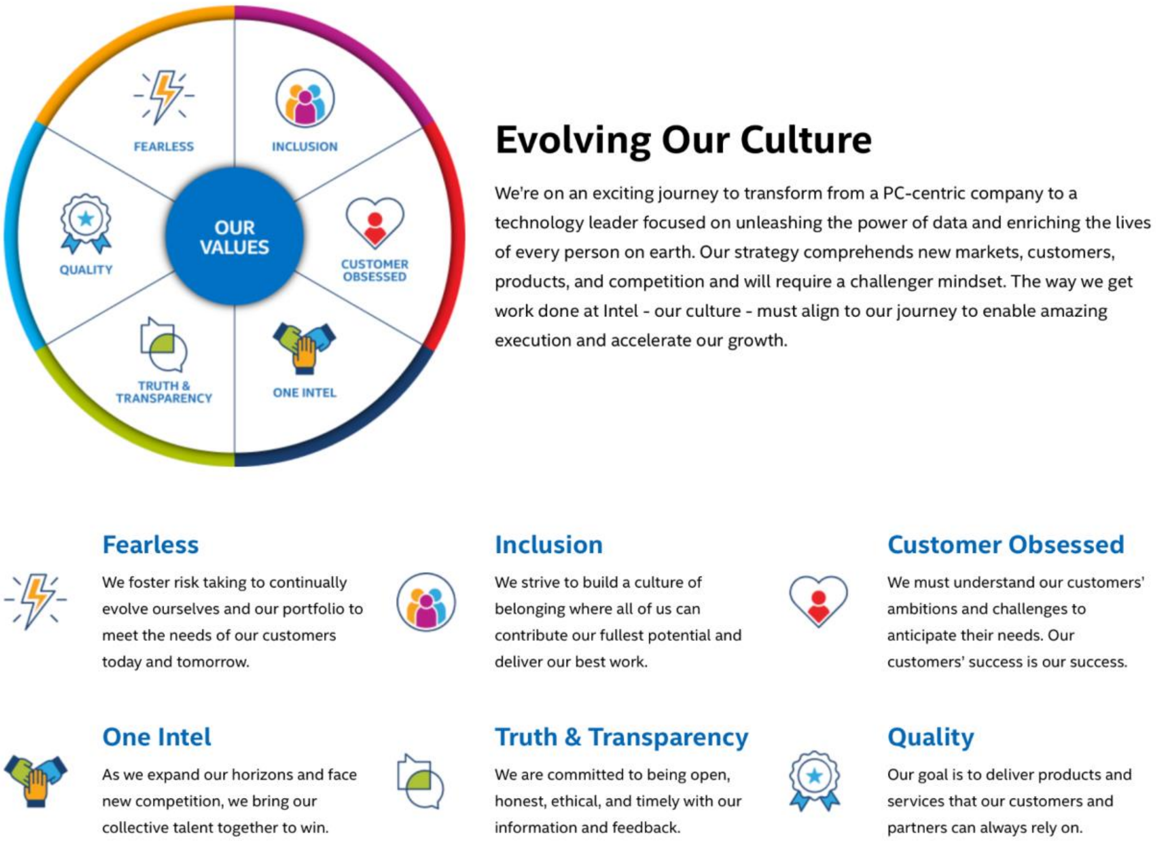
Company Overview

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' most significant challenges. By embedding intelligence in the cloud, network, edge, and every kind of computing device, we unleash the potential of data to transform business and society for the better.

Stock Overview
Symbol INTC Exchange Nasdaq
Market Cap Last Price 52-Week Range
123.27b $29.87 $24.59 - $56.28
11/18/2022 04:00 PM EST

Management Team Patrick Gelsinger
Chief Executive Officer
David Zinsner
Chief Financial Officer
Keyvan Esfarjani
Executive Vice President; Chief Global Operations Officer
Michelle Johnston Holthaus
Executive Vice President; General Manager, Client Computing Group
Dr. Ann B. Kelleher
Executive Vice President; General Manager, Technology Development
Raja Koduri
Senior Vice President; Chief Architect; General Manager, Architecture, Graphics, and Software
Greg Lavender
Chief Technology Officer; Senior Vice President, General Manager, Software and Advanced Technology Group
Nick McKeown
Senior Vice President; General Manager, Network and Edge Group
April Miller Boise
Executive Vice President and Chief Legal Officer
Christy Pambianchi
Executive Vice President and Chief People Officer
Matt Poirier
Senior Vice President, Corporate Development
Sandra L. Rivera

Executive Vice President; General Manager, Datacenter and AI
Christoph Schell
Executive Vice President; Chief Commercial Officer
Prof. Amnon Shashua
Senior Vice President, President, and CEO of Mobileye, an Intel Company
Sunil Shenoy
Senior Vice President; General Manager, Design Engineering Group
Dr. Randhir Thakur
Senior Vice President; President of Intel Foundry Services; Chief Supply Chain Officer
Shlomit Weiss
Senior Vice President; Co-General Manager of the Design Engineering Group
Safroadu Yeboah-Amankwah
Senior Vice President; Chief Strategy Officer



Evolving Our Culture

We're on an exciting journey to transform from a PC-centric company to a technology leader focused on unleashing the power of data and enriching the lives of every person on earth. Our strategy comprehends new markets, customers, products, and competition and will require a challenger mindset. The way we get work done at Intel - our culture - must align to our journey to enable amazing execution and accelerate our growth.

Fearless

We foster risk taking to continually evolve ourselves and our portfolio to meet the needs of our customers today and tomorrow.

Inclusion

We strive to build a culture of belonging where all of us can contribute our fullest potential and deliver our best work.

Customer Obsessed

We must understand our customers' ambitions and challenges to anticipate their needs. Our customers' success is our success.

One Intel

As we expand our horizons and face new competition, we bring our collective talent together to win.

Truth & Transparency

We are committed to being open, honest, ethical, and timely with our information and feedback.

Quality

Our goal is to deliver products and services that our customers and partners can always rely on.

Figure 1 (Intel Company Culture)

Intel's Operating Segments

At Intel, they have evolved alongside data. They have transformed beyond a PC-centric company to have a stronger focus on data, allowing them to address the needs of a new data-centric world.

Intel's segment reporting aligns with our organizational structure and business strategy. Beginning with their Q1'22 results, they will report results under six business units: Client Computing Group (CCG), Datacenter and A.I. Group (DCAI), Network and Edge Group (NEX), Accelerated Computing Systems and Graphics Group (AXG), Intel Foundry Services (IFS), and Mobileye (MBLY). This reporting structure enables transparent accountability relative to how well they manage and execute against the six business units.

Their main businesses include:

Client Computing Group
CCG creates platforms designed for end-user form factors, focusing on higher growth segments of 2-in-1, thin-and-light, commercial, and gaming, and growth opportunities in areas such as connectivity.

Datacenter and A.I. Group

DCAI focuses on developing leadership data center products, including Intel® Xeon® server and field programmable gate array (FPGA) products, and driving the company's overall artificial intelligence (A.I.) strategy.
Data-centric Businesses

Network and Edge Group

NEX is chartered with driving technology and product leadership throughout the network to the intelligent edge.

Accelerated Computing Systems and Graphics Group

AXG delivers high-performance computing and graphics solutions across clients, enterprises, and data centers.

Intel Foundry Services
IFS is a fully vertical, standalone foundry business that offers a wide range of manufacturing services to meet unique product needs, including our industry-leading sort and test capabilities.

Mobileye
Mobileye is a global leader in driving assistance and self-driving solutions. Our product portfolio covers the entire stack required for assisted and autonomous driving.

Data Center Group (DCG)
Internet of Things (IOTG)
Mobileye
Non-volatile Memory Solutions Group (NSG)
Programmable Solutions Group (PSG)

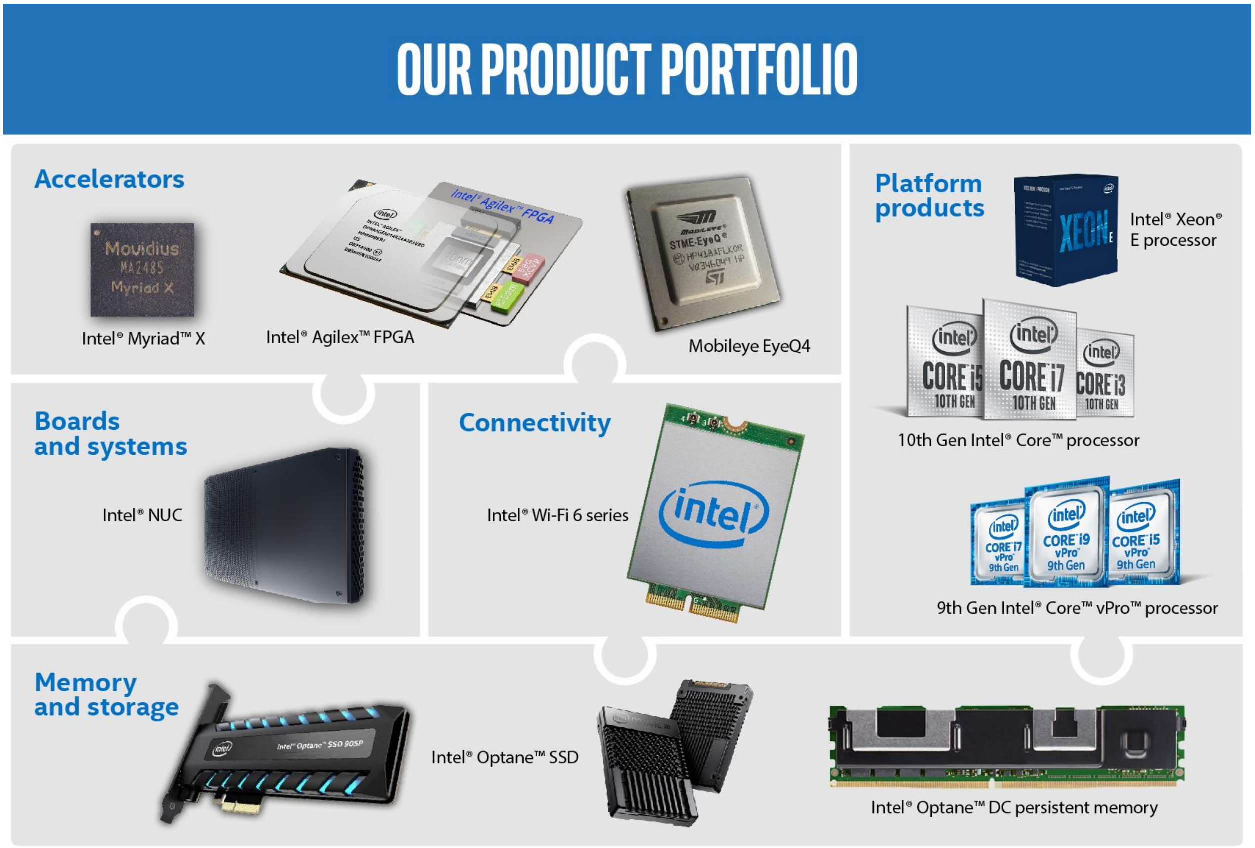


Figure 2 (Intel Businesses)

A Portfolio with Broad Market Potential

Their product portfolio (Figure 2) provides end-to-end solutions that address the needs of an ever-evolving data-centric world. In addition, Intel continuously develops new technologies and products for a broad spectrum of markets. From edge computing to the 5G network, cloud computing, A.I., and autonomous driving, our products deliver the necessary building blocks for an increasingly smart and connected world.

A Hardware Foundation for Government Cybersecurity

A proactive, hardware-based end-to-end strategy is needed to defend against the escalating threats to government cybersecurity. Every digital point, from the edge to the network to the cloud, will be protected with the support of this trusted infrastructure. In addition, solutions for data security and privacy are supported by Intel® hardware-enabled security technologies.
A secure government technological infrastructure supports the provision of critical services. These include disease management and prevention to assure health and well-being, local public safety, national security to protect residents, and transportation to keep business flowing. Along with safeguarding government data and algorithms, a sound cybersecurity plan also aids in protecting the personal information of individuals, a growing worry as organizations use more A.I. models.

Foreign and indigenous cybercriminals frequently attack public sector technologies. Viruses, Trojan horses, phishing, distributed denial of service (DDOS) assaults, illegal access, and control system attacks are a few of the instances that fall under this category. Cybercriminals want to steal money and information and stop the supply of vital public services. According to the U.S. Government Accountability Office, U.S. federal agencies reported more than 35,000 cyberattacks in 2017 alone. 1

Three reasons have increased cyber dangers for governments globally in recent years. First off, the assault surface keeps growing. That is partly because of the rising number of IoT devices, which is predicted to reach 30.73 billion by 2020. 2 Second, security software and firewalls that may have previously been successful are starting to be avoided by cyber attackers. Third, dispersed cybersecurity solutions offer openings that expose data to risk.
A proactive, end-to-end strategy that addresses five critical areas, according to our experts at Intel, is the ideal approach to cybersecurity:

- Threat detection and threat intelligence
- Data and application security
- Identity access management
- Network security
- Host and system security

There has never been a more pressing need for all security-related components to function together, including operating systems (O.S.), software, firmware, and hardware. For example, the

National Institute of Standards and Technology reports that firmware vulnerabilities are a growing target for cyberattacks (NIST). 3 Data encryption and O.S. security are no longer sufficient software defenses. Federal executive branch civilian agencies reported over 35,000 security events to the U.S. Department of Homeland Security in 2017. incidents to the U.S. Department of Homeland Security.

Intel® Hardware-Enabled Security Technologies

In the cybersecurity defense of the state, local, and federal governments, hardware-based security capabilities may be crucial. From the endpoint, which might be a laptop, security camera, drone, or another piece of equipment placed in the field, through the network and to the data center and cloud, they can aid in protecting data and devices.

Security capabilities enabled via hardware are a pillar of Intel® products and technology. We build specialized hardware and software to protect data from cyberattacks and incorporate security measures into our products.

P.C. Client Security

The Intel vPro® platform offers hardware-enhanced security measures and quick response times for commercial computing. It has technologies like Intel® Hardware Shield, which offers improved defenses against assaults underneath the O.S. and cutting-edge threat detection capabilities for heightened platform security. Even in power loss or O.S. failure situations, Intel® Active Management Technology's remote detection and recovery saves time and lowers on-site support expenses.

Their silicon includes Intel® Threat Detection Technology (Intel® TDT) to improve the services offered by unaffiliated software providers. Existing capabilities are improved, and cyber threats and exploits are better detected thanks to Intel® TDT.

Intel® Security Essentials

Intel® Security Essentials deliver a hardware trust foundation. This supports dedicated apps and safeguards platforms and data without sacrificing performance:

Applications can execute in their areas thanks to separated enclaves made possible by Intel® Trusted Execution Technology (Intel® TXT).

The foundation of platform trust and security services is the hardware-assisted acceleration of computationally intensive cryptographic procedures.

Platform integrity comes from a protected and validated boot process with hardware attestation. Saved data, keys, and identity help assure encryption and storage for sensitive information at rest and in transport and prevent abuse or exposure.

Internet of Things Security

IoT security must cover hundreds or thousands of connected devices and the big data they generate. Intel advocates integrating security into IoT solutions, starting with the computing device. Advanced hardware and software can help prevent harmful applications from being activated on a device or from taking down a network.

We work with our partners in the IoT ecosystem to design solutions with security in mind. Intel® IoT Market Ready Solutions (Intel® IMRS) are scalable, repeatable, end-to-end solutions available now. They are designed specifically for healthcare, smart cities, and other public and private sector markets. Intel® IoT RFP Ready Kits help solve industry-specific challenges with bundled hardware, software, and support. OEMs, ODMs, ISVs, and distributors develop these kits on a foundation of Intel® technologies.
Network Security

Intel® QuickAssist Technology (Intel® QAT) delivers a highly efficient network and software-defined infrastructure (SDI). It provides acceleration for security, authentication, and compression algorithms for high performance in data center and cloud systems. Accelerating SSL/TLS with Intel® QAT enables:

· High-performance encrypted traffic throughout a secured network
· Compute-intense symmetric and asymmetric cryptography
· Platform application efficiency

Intel® QAT delivers performance across applications and platforms. This includes symmetric encryption and authentication; asymmetric encryption; digital signatures; RSA, D.H., and ECC cryptography; and lossless data compression.

Data Center and Cloud Security

Government systems increasingly rely on the cloud and virtualized infrastructure comprised of virtual machines (V.M.), containers, or both.

Intel® technologies such as Intel® TXT, Intel® Security Libraries for Data Center (Intel® SecL - D.C.), and the recently announced Intel® Converged Boot Guard. Trusted Execution (Intel® CBnT) provides trusted infrastructure capabilities for cloud, virtualized, and containerized environments. Intel® TXT and Intel® SecL - D.C. provide scalable security controls enabling trusted boot and attestation to the authenticity of the platform configuration, BIOS and O.S./virtual machine monitor (VMM), and even guest environments. In addition, Intel® CBnT adds integration with Intel® Boot Guard to Intel® TXT to provide verified boot capabilities for servers.

Intel® Resource Director Technology (Intel® RDT) brings heightened visibility and control over how applications, V.M.s, and containers use shared resources. Intel® RDT monitors usage to allocate resources intelligently and ensure no application is unexpectedly monopolizing the system.

Modern data centers built upon silicon-based trusted infrastructure can better consolidate servers, allow distributed virtualization, and support private and hybrid clouds. In the data center, Intel® Software Guard Extensions (Intel® SGX) help protect application integrity and data confidentiality. At the same time, Intel® AES New Instructions (Intel® AES-NI) speeds up data encryption to help protect data at rest and in transit without performance penalties.
Data centers powered by Intel® Xeon® Scalable processors help reduce costs while supporting cloud security. In addition, Intel® Cloud Integrity Technology (Intel® CIT) helps ensure cloud applications run on trusted, unaltered servers and V.M.s. Thanks to an ancestral root of trust, Intel® CIT can attest to integrity and compliance across cloud computing pools.

Supply Chain Security

Today's supply chains are complex, far-flung, and focused on speed and cost. Intel is committed to improving the integrity and traceability of Intel® products throughout their life cycles. Compute Lifecycle Assurance (CLA) is an industry-wide effort to establish an end-to-end framework to improve transparency from build to retirement. CLA can help improve platform integrity, resilience, and security.

The Intel® Transparent Supply Chain (Intel® TSC) is a set of policies and procedures implemented at our manufacturers' factories. These enable our customers to validate where and when components of a platform were manufactured.

Intel Policies

Security and Trust Policy - Intel uses coordinated vulnerability disclosure processes and collaborates with industry, academia, and independent researchers.
Intel's security objective is in direct alignment with the goal of global governments, which is to promote trust in technology by enabling governments, businesses, and individuals better to

secure their data, networks, and infrastructure. Intel plans on accomplishing this goal by inspiring governments to be aware of non-partisan methods of protection to foster statistics-era innovation and monetary growth. Intel further explains how Governments need to promote regulations that might be globally scalable and flexible enough to cope with the evolving protection panorama with the aid of using software that specializes in sturdy and transparent protection solutions. In addition, Intel believes they need to increase risk-based, evidence-driven, design-impartial methods to protect coverage and be knowledgeable using consensus-driven processes.

Intel believes that to develop sound cybersecurity policies, they need to urge governments to focus broadly on advancing policies that target mutually beneficial outcomes, such as

- Improve industry and government information sharing in a way that protects business liability while maintaining data confidentiality, integrity, and availability.
- Encourage cybersecurity research, development, and workforce development. Encourage reliable, transparent, and resilient supply chains.
- Create security policies built on a solid foundation of internationally recognized best practices, standards, and technologies, while allowing for flexibility for ongoing innovation and growth.

There are some key issues Intel identifies as high-level recommendations that would help guide their policy regarding security and trust. One of the critical issues lies within supply chain security.

Intel sees information and communications technology (ICT) supply chains increasingly targeted by sophisticated cyberattacks. Never before have these strikes had such a profound effect, especially in light of the SolarWinds attack and the COVID-19 epidemic. Instead of creating policies based on a foundation of evidence, data, and openness, countries are starting to prioritize policies targeting the country of origin to reduce supply chain risk. Purely unilateral supply chain policies, especially in the United States (U.S.), are likely to have reciprocal repercussions on other countries, having a considerable detrimental influence on global trade. Governments should support policies prioritizing domestic manufacturing investment while providing clear, open rules and guidelines for protecting global supply chains rather than erecting obstacles to developing a healthy global supply chain. Trust-based, objective standards (such as those developed by the DHS Supply Chain Risk Management Task Force) are more enduring and less likely to be impacted by political movements that lead to nation-specific exclusions.

Another critical issue Intel sees as a high-level recommendation is 5G Security. Intel has consistently backed legislation that supports reputable 5G solutions built on openness and technological standards. As supply chain issues and 5G become more interconnected, lawmakers must consider both when writing legislation. Intel supports initiatives like Open RAN, which is viewed globally as a chance for nations to create new businesses and market entrants to bring out 5G. Intel supports a 5G policy that aims to provide a secure, dependable, and open infrastructure because 5G will be a part of the global.

Encryption is a significant consideration from Intel for trust and security.
They believe encryption is a vital technology required for secure and dependable ICT infrastructure. In previous decades, scholars, businesses, and governments from all over the world worked together to create encryption techniques that facilitated interoperability on a global scale. Unfortunately, the compatibility of the global market is harmed by local technology regulations that are suggested in the guise of national security. Moreover, such requirements may have a detrimental effect on users there since they make technology less safe by default. For this reason, Intel favors globally harmonized encryption standards and laws.

Security Certifications play a significant role in Intel's critical issues with their Security and Trust policy. They believe that To promote consumer confidence in the goods, services, and businesses operating in their marketplaces, governments worldwide are becoming more interested in developing cybersecurity certification and labeling programs. The E.U. Cloud Certification Scheme, NIST FIPS 140-3 Security Requirements for Cryptographic Modules, and several additional ideas are now under consideration. Intel supports government initiatives to guarantee acceptable security for its products, provided that these initiatives use a risk-based approach to identify the necessary standards and can change at the speed of technological innovation. Intel believes the optimal way to safeguard the environment depends on the context of technology deployment, as is underlined in ITI's Policy Principles for Cybersecurity Certification. Often, blanket criteria are too strict about accounting for this variation. Additionally, technical innovation develops quickly, and certification programs must frequently catch up with new advances. Before adopting a certification or labeling regime, all of these and other variables must be considered. Finally, the establishment and maintenance of the long-term success of such a plan depend on collaboration with the industry during its development.

Lastly, Intel believes securing Internet of Things (IoT) devices would help with their Security and Trust policy. Ubiquitous connectivity has ushered in a new era of intelligent, connected gadgets and data-driven capabilities that benefit society and people. Public policies should promote innovation and competition to maintain these advantages and hasten the deployment of a secure, scalable, and interoperable IoT. IoT security regulation proposals have been made globally in response to worries about growing attack surfaces and increased embedding in the digital ecosystem. Intel favors design-neutral regulations based on globally harmonized standards, use risk-based security strategies for IoT devices, prevent fragmented requirements, and promotes interoperability. Intel actively participates in the ecosystem in the creation of international standards in ISO (JTC 1, SC27) and other organizations. Additionally, Intel takes part in consensus-driven initiatives, such as the Council to Secure the Digital Economy's C2

Consensus on IoT Security Baseline Capabilities project and the NIST IoT Device Security Requirements (NISTIR 8259).

Public Privacy Policy

Intel's data privacy policy approach aims to increase consumer and societal trust in technology by allowing responsible access to and use of data. Intel urges governments to concentrate on unified privacy protection strategies that will continue to support information technology innovation and economic growth to achieve this aim.

Key Issues

Global Interoperability: The free flow of information and innovation should be encouraged by privacy laws. Free trade agreements and other policy efforts should not impose protectionist restrictions on data mobility.

Risk-Based Approach to Innovation: Laws governing privacy should be flexible and based on a risk-based methodology. Intel supports adopting privacy legislation that tackles the issues and dangers brought on by developing new and existing technologies. In addition, lawmakers should support Privacy by Design and organizational responsibility for balancing privacy risks throughout data lifecycles.

Harmonized Regulation: Intel favors a comprehensive federal privacy law being passed in the U.S. Inconsistent rules could be imposed by a patchwork of potentially incompatible state or sectoral privacy laws, hurting consumers and technological innovation.

Security and Privacy: Intel states how good privacy requires security. Data sharing and storage requirements will increase as more digital devices are connected to the internet. Therefore, device and network security must be robust. Any privacy law must consider network and information security concerns while processing data.

Enforcement: Enforcement of data privacy laws must be predictable and consistent in order to meet consumer expectations.

CyberSecurity Policy

The Future of Cybersecurity

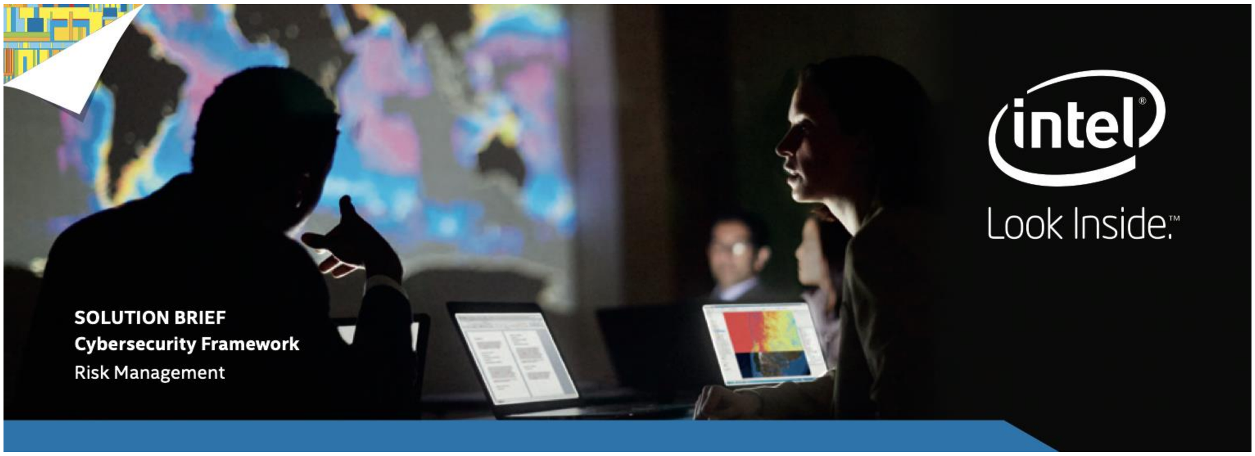


Figure 3 (CybersSecurity Framework)

Government institutions, public sector organizations, and technology companies are reexamining their approach to protective measures in security and privacy. As the threat landscape evolves, our commitment to product security at Intel will remain a critical priority. Our engineers and security experts will continue to work together to design products that promote a robust and resilient cyberspace.

Intel supports privacy and cybersecurity laws and regulations that will increase public confidence in Intel's technology and products while also assisting businesses, organizations, and individuals in strengthening the security of their networks, data, and intellectual property. We recommend governments concentrate on bipartisan consensus strategies to enhance cybersecurity and privacy while supporting I.T. innovation to achieve these goals. We have argued against regulatory strategies for vital supply chains or infrastructure that could influence product development and potentially set unfavorable precedents. Intel asks the government to concentrate on the following in order to develop a robust cybersecurity policy:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework should have congressional backing. Intel applauds the government and NIST for collaborating with industry and other stakeholders to develop the cybersecurity framework to create a prototype for a voluntary, risk-based tool that a wide range of public and private sector entities can use.

- Cybersecurity should not be used as justification for protectionist laws. According to Intel, the production method, not the location, should determine the reliability of technological products. Leading international technology company Intel opposes laws that bar businesses from specific markets based on where they were founded. Intel fears such legislation may serve as a model for laws elsewhere, hurting U.S. businesses. Any cybersecurity law, rule, guideline, or policy should provide proper privacy safeguards and act as a valuable model for other nations.

- To foster trust, legislation governing governmental access to data from the private sector must be updated. More work needs to be done to boost confidence and trust in technology use. In order to achieve this, the public and private sectors must work together, and the government, businesses, and other affected stakeholders to deliberate carefully. The Modernization of the Electronic Communications Privacy Act and the Digital Due Process Coalition are initiatives supported by Intel. The company also thinks that the Foreign Intelligence Surveillance Act (FISA) surveillance laws can be improved to maximize economic security, individual privacy, and national security interests.

Regulatory Compliance and Beyond

Intel complies with all applicable regulations, and Intel Environmental Health & Safety (EHS) requirements wherever we operate. We proactively engage with stakeholders to develop responsible laws, regulations, and innovative programs that provide safeguards for the community, the workplace, and the environment, while allowing flexibility to advance our technologies. We recognize the importance of EHS to business success, and we are committed to continually improving our EHS Management System, including standards, culture, performance, and injury reduction initiatives.

Safety and Health

Intel's commitment is to provide a safe and injury-free workplace for all our employees, contractors, customers, partners, and the public. We are constantly assessing and improving our EHS programs and training to increase our focus on prevention, early intervention & safety culture. We continue to strive to integrate safety into our daily business and to encourage responsibility for our own & others' safety. We promote a healthy lifestyle and proactively encourage employees to manage their health and wellness.

Environmental Sustainability

Intel strives to be a global leader in sustainability and environmental protection, enabling our customers and others to reduce their environmental impact through our actions and technology. Intel identifies vital environmental aspects of our operations and mitigates impacts by incorporating circular economy principles. Intel will continue to invest in conservation; we will work to reduce our environmental footprint and adhere to our environmental policies (climate, water, and energy) and RISE goals.

Public Information Transparency

We are responsible members of the communities in which we live and work. As we expand our knowledge and understanding of the impact of our operations and our products, we share this knowledge with the broader community to increase awareness of the importance of environmental issues. We transparently establish and regularly report on our RISE EHS related goals and metrics.

Supplier and Contractor Relationships

Intel holds suppliers accountable for the exact expectations we have for ourselves. We are committed to advancing accountability and improving EHS performance through proactive communication, assessments, and capability-building programs. We set high safety training and performance expectations during our contracting process and orientation for new on-site suppliers. We partner with our chemical and gas suppliers on green chemistry initiatives and with general suppliers on environmental, health, and safety initiatives.

Emergency Preparedness

We proactively evaluate our risks, coordinate periodic testing, and learn from previous situations to continuously improve our processes and be prepared to respond to emergencies that could impact the health & safety of employees, the environment, our operation

Security and Trust Policy

Intel's security objective is directly aligned with the goal of global governments to promote trust in technology by enabling governments, businesses, and individuals better to secure their data, networks, and infrastructure. We encourage the government to focus on non-partisan approaches to foster information technology innovation and economic growth to accomplish this goal. Intel believes in developing risk-based, evidence drive, design-neutral approaches to security policy and being informed by consensus-driven processes.

Automotive and Transportation Policy

Intel is a market leader in automation systems for driver assistance, with over 60 million vehicles on the road around the world today. This foundation of leadership in advanced driver assistance systems (ADAS) makes Intel uniquely knowledgeable about the life-saving capability of vehicle automation technologies. In addition, through our Mobileye division, Intel will be a global leader in the delivery of self-driving systems. As a result, we are positioned to make autonomous driving a reality. In addition, we have the collective depth and breadth of experience, talent, technology, and resources to deliver safe and scalable A.V. solutions.

Digital Health Policy

Healthcare systems are embracing the transformative power of technology. For example, electronic health records organize medical data and enable providers to share it more easily across healthcare settings. In addition, artificial intelligence (A.I.) helps physicians and researchers prevent disease, speed recovery, and save lives, while telehealth improves the experience, access, and speed of care.

Technologies like A.I., robotics, and the Internet of Things (IoT) make healthcare and life sciences more connected, personalized, and intelligent.

Privacy Policy

Intel recognizes that innovation success depends upon individuals' trust in their technologies, particularly with emerging technologies like artificial intelligence (A.I.) and autonomous driving. Intel believes that robust privacy protection is a critical component of consumer awareness and trust and works with governments worldwide to engage in meaningful discussion about approaches to data privacy legislation.

Digital Trade Policy

Intel is working relentlessly to unleash the potential of data, leading to more capable and efficient networks and pervasive connected, intelligent devices. Moore's Law set the pace for the digital revolution and continues to inspire us today. Data is not only a means of production; it is also an asset that can be traded and a means through which global supply chains are organized and services delivered. It also underpins physical trade by enabling the implementation of trade facilitation. Data is also at the core of new and rapidly growing service supply models such as cloud computing, the Internet of Things (IoT), and Artificial Intelligence (A.I.). Intel believes that data is dramatically shaping the future of all humankind and driving innovation at a record pace.

Benefits of Intel's cybersecurity policies:

- Improved industry and government information sharing to maintain data confidentiality, integrity, and availability with adequate liability protection to a business.
- Promote cybersecurity research and development (R&D) and workforce development.
- Support trustworthy, transparent, and resilient supply chains.
- Design security policy that rests on a robust foundation of internationally recognized best practices, standards, and technologies, while allowing flexibility for continuous innovation and growth.

Critical Issues for Intel Corporation

Supply Chain Security: Cyberattacks against information and communications technology (ICT) supply chains are becoming very sophisticated. These attacks were never more significant than during the COVID-19 pandemic and Solar Wind attacks. Countries are beginning to favor policies that target the country of origin to mitigate supply chain risk rather than developing policies built on a foundation of evidence, data, and transparency. Purely insular supply chain policies, particularly in the United States (U.S.), likely have common effects with other nations, causing significant negative impacts on international trade. Rather than creating barriers to building a robust global supply chain, governments should support policies focusing on domestic production investment while establishing clear, transparent standards and guidelines for securing global supply chains.

5G Security: Intel has long supported policy that favors trusted 5G products grounded in transparency and technical standards. The relationship between 5G and supply chain challenges is increasingly intertwined, so policymakers need to be conscious of both areas when drafting policy. Intel supports efforts like Open RAN, which is seen internationally as an opportunity for countries to build new companies and new market entrants to roll out 5G. Since 5G will be a part of the global internet infrastructure, Intel supports a 5G policy that seeks to ensure safe, reliable, and open infrastructure.

IoT Devices: Ubiquitous connectivity has brought forth a new era of intelligent, connected devices and data-driven capabilities delivering benefits to society and users. Public policies should encourage innovation and competition to preserve these benefits and accelerate secure, scalable, and interoperable IoT deployment. Concerns regarding expanding attack surfaces and increased embeddedness in the digital ecosystem have prompted IoT security regulation proposals globally. Intel supports design-neutral regulation rooted in internationally harmonized standards that leverage risk-based approaches to securing IoT devices and avoid fragmented requirements while supporting interoperability.

· Security Certification: Governments worldwide show increased interest in creating cybersecurity certification and labeling schemes to boost confidence in products, services, and companies in their markets. Current proposals include the E.U. Cloud Certification Scheme, NIST FIPS 140-3 Security Requirements for Cryptographic Modules, and several others. Intel supports government efforts to ensure adequate security for its technologies as long as they follow a risk-based process for determining appropriate requirements and can evolve with technological advancement. The context for technology deployment is critical to determining how best to secure the environment (highlighted in ITI's Policy Principles for Cybersecurity Certification). Blanket requirements are often too rigid to accommodate this variance. Additionally, innovation in the technology space evolves rapidly, and certification schemes often cannot keep pace with new developments—all these factors and more need to be considered before pursuing a certification or labeling regime. Collaboration with industry during the development of such a scheme is vital to establishing and maintaining long-term success.

Encryption: Encryption is a fundamental technology that makes ICT infrastructure secure and reliable. In past decades, researchers, industry, and governments collaborated to develop encryption mechanisms supporting global interoperability. Local technology mandates proposed in the name of national security cause harm to the compatibility of the global market. Such mandates can negatively impact users within that country by forcing the technology to be, by nature, less secure. For this reason, Intel supports globally harmonized encryption standards and regulations. See more in this blog that details Intel's positions on encryption policy.

Cybersecurity should not provide a rationale for protectionist policies. Intel believes the trustworthiness of technology products should be based on how they are made instead of where they are made. As a leading global technology company, Intel advocates against legislation that excludes companies from markets based on the company's country of incorporation. Intel is concerned that such legislation in the United States might spur legislation elsewhere, which would negatively impact U.S. companies. Any cybersecurity legislation, regulation, standard, or policy should include adequate privacy protections and serve as a valuable template for action by other countries.

Modernizing legislation governing government access to private sector data is necessary to build trust. However, more needs to be done to increase trust and confidence in using technology. Doing so requires private sector innovation and government policies that focus on public-private collaboration and thoughtful deliberation by government, industry, and other impacted stakeholders. Intel supports the Digital Due Process Coalition and modernization of the Electronic Communications Privacy Act and believes practical reforms to Foreign Intelligence Surveillance Act (FISA) surveillance laws that optimize for national security, individual privacy, and economic security interests can help build trust and serve as a useful guide for other countries.

Congress should support the National Institute of Standards and Technology (NIST) Cybersecurity Framework approach to improving cybersecurity. Intel commends the administration and NIST for constructing the cybersecurity framework hand-in-hand with industry and other stakeholders to build a model of a voluntary, risk-based tool that a broad array of public and private sector organizations can utilize.

Congress should make progress on consensus areas. Intel asks Congress to advance legislation targeting areas of bipartisan consensus: (1) sensibly improving industry and government information sharing in a way that ensures privacy is protected, offers adequate liability protection to business, and promotes continued innovation; (2) promoting cybersecurity research and development (R&D) and workforce development; (3) strengthening the security of government networks through Federal Information Security Management Act (FISMA) reform; (4) strengthening criminal penalties for cybercrimes.

RESOURCES

A cybersecurity framework use case Intel Corporation. (n.d.). Retrieved November 21, 2022, from https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf

Strategic priorities. Intel Corporation. (n.d.). Retrieved November 21, 2022, from https://www.intc.com/strategic-priorities