OCTOBER 2024

Trusted Chips

Why the Discussion Risks Distracting from Solving Policy Issues

By Andreas Schumacher

Introduction

The United States and its allies have taken significant actions to promote the de-risking of semiconductor supply chains. Protecting and controlling these supply chains also remain critical components of national and economic security discussions. To achieve this holistically, several sometimes-conflicting goals need to be met:

1. Critical technologies and products need to be controlled.
2. Export control sanctions must be enforced.
3. Sensitive information must be safeguarded against attacks through compromised chips.
4. Overreliance on nonmarket actors must be avoided.
5. A competitive, commercially viable semiconductor supply must be ensured.

Many of these policy goals have been recently subsumed under a general call for “trusted” or “trustworthy” chips. In reality, the goals are varied and complex, and trade-offs are unavoidable. For example, adding security features will increase costs and might not be technically feasible for most semiconductors.

Without specific, clearly defined, and aligned policy goals—along with an appreciation of the technological boundary conditions and an understanding of the economic impacts along the supply chain—the discussions among the United States and its allies are unlikely to yield meaningful results. “Trusted chips” will continue to mean different things to different stakeholders, detracting from solving the underlying issues.

This white paper offers three recommendations for policymakers to address pertinent questions about the semiconductor supply chain:

1. Align on specific policy objectives rather than definitions.
2. Use, refine, and align existing policy tools devised for specific objectives.
3. Enable and seek industry involvement to ensure commercial viability and promote fast adoption.

Mapping Wide-Ranging Policy Objectives onto a "Trusted Chip" Concept Will Fail

Security typically deals with technical controls and processes, whereas trust is a social concept that goes a step further: It is fundamentally about relationship dynamics and the expectations that come with them.

The term "trusted chip" thus sets a high bar. It might imply, for example, the confidence that the semiconductor will perform according to its specifications under all conditions and be free of unintended defects or malicious manipulation. It could also signal awareness or control over the product's provenance—transparency about the chip's exact supply chain, or at least certainty that critical steps in the supply chain took place outside the control of adversaries.

Among semiconductor industry experts, the term "trust" historically means one of two narrowly defined concepts:

Trusted Microcontrollers

A dedicated microcontroller (MCU), or parts of an MCU designed to secure hardware through integrated cryptographic features, is called a Trusted Platform Module (TPM).[1] TPMs have proliferated from sensitive defense or government applications to high-volume consumer devices such as personal computers and mobile phones. An **ISO/IEC 11889 standard** was published in 2009. Trusted MCUs are instrumental in achieving high system-level cybersecurity standards, such as those called for by the **U.S. Cybersecurity Label** for consumer and Internet of Things devices or the European Union's **Cyber Resilience Act**.

Trusted Supply Chains

In 2003, the U.S. Department of Defense initiated a Trusted Foundry Program, now part of the Defense Microelectronics Activity (DMEA)'s **Trusted Supplier Program**. As of early 2024, **16 out of 82** accredited trusted suppliers were also accredited for semiconductor foundry services, to provide services for advanced and foundational chips. The program is tailored to critical but less cost-sensitive defense and national security applications.

The two concepts can be applied simultaneously. However, while the latter can be applied to all semiconductors, the former is limited to a specific product category.[2]

There are more recent attempts to broaden the concept of trusted semiconductors. Examples can be found in the 2023 **European Chips Act**, which advocates for "trusted, secure and green chips." However, a clear definition remains elusive.

[1] Hardware security modules, secure enclaves, and secure elements/hardware roots of trust offer the same function.

[2] Trusted supply chains are, in principle, limited by the foundries' technology offerings.

In the context of controlling access to the most advanced artificial intelligence (AI) hardware, **secure and governable AI chips** have been proposed, expanding on the concept of trusted MCUs.

Some policymakers even proposed the concept of trusted semiconductors as a trade remedy–that is, restricting access to U.S. and allied markets to trade with trusted chips. Lastly, it has been suggested that trusted chips could aid in verifying export control compliance.

This short overview illustrates how the concept of trust, broadly applied to semiconductor markets, glosses over crucial details: Should it apply to all chips or only some? Should it benefit broad consumer markets or defense contractors? Do the costs of implementing a technical solution matter or not? Mapping wide-ranging policy objectives–such as export control, supply risk mitigation, trade policy, cybersecurity, and integrity of critical microelectronic systems–onto the "trust" concept is bound to fail. Worse, it will distract from meaningful discussions.

Answering Four Questions Can Structure and Focus the Discussion

Policy solutions to guide semiconductor export control, supply risk mitigation, trade policy, and cybersecurity are nevertheless pertinent. They need to be coupled with an appreciation for technological feasibility and private sector commercial incentives.

Answering four questions will help to structure and focus the discussion (Figure 1).

Figure 1: Option Space for Key Semiconductor Policy Questions

Range of Options ⟷

1. Which semiconductors to cover?	• Microcontrollers and processors • Allows on-chip implementation of security features and traceability with limited cost overhead		• All semiconductors (e.g., power semiconductors, RF chips) • Limited to no ability for embedded security • On-chip traceability with high cost added
2. Which systems to cover?	• Low-volume critical systems (e.g., military, crypto, government ID)	• Mid-volume public and corporate infrastructure	• High-volume electronic systems (e.g., personal electronics, IoT devices, cars)
3. What are policy requirements?	Chip or system level: • Export control • System/data protection • Trade remedies		Supply-chain level: • Resilient commercial supply chains • Supply chain transparency • Tight supply chain control
4. Commercial viability?	• Limited relevance (e.g., government buyers for limited-volume critical systems)	• Commercial market, buyer does not accept premiums for de-risking supply, security, etc.	• Commercial Market, buyer accepts premiums for availability, security, etc.

Source: Author's research.

1. **Which semiconductors should be covered?** MCUs and microprocessors (MPUs) allow, in principle, the implementation of on-chip security features to establish trust, traceability, and, potentially, governance features. However, MCUs and MPUs combined cover less than **15 percent** of the semiconductor market. On-chip security features are not technically feasible for much of the remaining 85 percent (e.g., sensors, power semiconductors, other discrete semiconductors). These devices lack the compute and memory capabilities to execute trust functionality.

   A unique, tamper-proof, chip-level identification for all semiconductors would be commercially prohibitive in most cases. Printing a unique marker on every semiconductor's packaging would be cheaper, but it would still need to be backed by an industry-wide global database to detect misuse reliably.

2. **Which systems should be covered?** Critical applications—such as military command, control, communications, and computing equipment—require the highest technical level of device security and supply chain provenance. Additionally, the export of these application-specific or dual-use chips to adversaries often needs to be controlled. At the same time, the universe of parties that are affected by stringent requirements is relatively small: government agencies or prime contractors as buyers and a small number of accredited suppliers. Their willingness to shoulder the additional compliance and risk mitigation costs is high.

   Another example involves high-volume consumer devices, which can indeed provide a high level of trust. For instance, a laptop or mobile phone must protect personal information and securely execute payment transactions. While this can be achieved with on-chip hardware security (available to retail consumers as aftermarket products for **less than $30**), full end-to-end control of a mobile phone or laptop supply chain is not commercially viable. For instance, one major U.S. consumer electronics company's **supplier list** includes 200 suppliers with 600 sites at locations across the globe.

   Basic connected consumer devices often fall short of any digital security standards, something the **EU Cyber Resilience Act** and the **U.S. Cybersecurity Label** seek to address.

3. **What are the policy requirements?** After deciding which parts of the semiconductor market and which systems should be covered, policymakers need to agree on who or what they are trying to protect and what degree of certainty constitutes success in achieving their goals.

   At the level of a single chip or microelectronic system, policy goals might include the control of exports and protecting the system (or data) from unauthorized access or manipulation. Alternatively, labeling trusted semiconductors could serve as a trade action in disguise to restrict imports from suppliers or countries engaging in nonmarket state practices and policies.

   At the level of the entire supply chain, policy goals may include the reliable supply of commercial semiconductor goods and supply chain transparency. In the case of the U.S. Department of Defense's Trusted Supplier Program, the goal is very tight control over every step of the semiconductor supply chain.

   Along with these requirements come different definitions of what constitutes success. Trade remedies might be considered successful at the 80 percent level, an export control agency might be satisfied with 95 percent compliance, and defense-critical applications could demand an even higher level of confidence in the integrity of the respective semiconductor supply.

4. **Is the solution commercially viable?** If governments procure trusted chips for critical applications, they can set the economic incentives directly and compensate suppliers for the costs of manufacturing and controlled supply chains. Suppliers can price in the opportunity cost of export controls, that is, the fact that application-specific products cannot be sold in certain markets.

   The economics will play out very differently in the case of high-volume consumer applications, where end customers may or may not be willing to pay a premium for security or availability. In those scenarios, governments must work closely with industry and gradually influence economic incentives to steer commercial actors toward policy goals.[3]

Answering these questions theoretically results in a large number of different scenarios. However, these scenarios can be distilled into a limited number of practical policy challenges—and the tools to address those challenges are often already available. Policymakers should focus on refining these tools and achieving better alignment among allies regarding their use.

Solve Practical Policy Challenges Instead of an Overarching Definition

In reality, solving practical policy challenges is less complex. **Semiconductor devices date back to 1947**, as do the challenges to safeguard the technology, protect critical electronic systems and sensitive information from unreliable or malicious chips, and ensure a commercially viable supply of semiconductors. Even the risks of overreliance and state-subsidized industrial production are not new—although the **scale of this risk** might well be.

A. **Critical Electronic Systems:** For national security reasons, the United States and its allies have long controlled the semiconductor supply chain for critical electronic systems, such as those used in defense applications. This may involve both hardware and supply chain solutions. Given the sensitive nature of the applications, tools like DMEA's **Trusted Supplier Program** are typically deployed on a national level. In addition to whitelisting trustworthy suppliers, blacklisting certain entities is an effective option with a strong forward-signaling impact. Examples include the **EU toolbox for 5G security** (though deployed with varying urgency among member states) and the more targeted **Section 5949** of the U.S. National Defense Authorization Act of 2023.

   Commercial viability can typically be achieved due to the limited scope of applications, semiconductor volumes, and involved parties.

B. **Cybersecurity of Electronic (Sub-)Systems:** This is another area where technical and commercially viable solutions either already exist (e.g., **ISO/IEC 11889** for secure crypto-processors, **ISO/SAE 21434** for automotive cybersecurity) or are being implemented (e.g., the **U.S. Cybersecurity Label** and the **EU Cyber Resilience Act)**. More recently, the U.S. government proposed a rule to secure information and communications technology for connected vehicles. The **rule** would regulate hardware "designed, developed, manufactured, or

[3] The $30 aftermarket upgrade for personal computers and laptops became compelling after Microsoft's Windows 11 Operating System required a Trusted Platform Module.

supplied by a person owned by, controlled by . . . the PRC or Russia." Effectively, a concept of "non-trusted" semiconductors is being established, though without explicitly calling it that.

Therefore, policy and commercial solutions are available or have been proposed for these use cases.

C. **Export Controls:** Limiting the export of certain types of semiconductors, their underlying technology, and manufacturing equipment is an established practice for the United States and its allies. New frameworks **might be needed** to address shortcomings of existing multilateral export control regimes. Still, in the meantime, multilateral, case-by-case agreements have been successfully achieved (e.g., the United States, Japan, and the Netherlands **reaching a deal** to curb chipmaking exports to China). Enforcing export controls for advanced AI MPUs is **challenging**, and stopping the illicit flow of legacy semiconductors to Russia is even harder. Solutions have been proposed to **improve export control compliance**, but introducing the concept of trusted MCUs or trusted supply chains is not among them. Export control is not an inbound issue–ensuring the United States and its allies get trusted products–but an outbound issue–ensuring adversaries do not obtain them.

D. **Supply Chain Provenance Law:** Various supply chain provenance requirements have been introduced in recent years. Examples include the **Uyghur Forced Labor Prevention Act** and the **Corporate Sustainability Due Diligence Directive**. In response to these requirements, companies–including semiconductor manufacturers–are implementing rigorous supply chain monitoring and verification systems, which, by definition, will apply to all their products. Introducing a "trusted chip" certification based on a geography- or entity-specific listing would be possible and might–considering the forward-signaling effect of various U.S. rulemaking proposals–already be expected by industry participants. Policymakers, however, need to carefully weigh the additional reporting burden on the industry against national and economic security goals.

E. **Trade Remedies:** There is **mounting concern** that Chinese industrial policy, including in the semiconductor market, supports domestic firms that do not operate according to market principles. The United States and its allies can use tools–principally tariffs–to counter nonmarket policies and practices. However, these remedies often amount to too little, too late, especially if lengthy negotiations among allies precede them.[4] Moreover, tariffs are applied to the end product entering a market–such as a computer, mobile phone, or industrial machinery control system. Relatively few chips enter the U.S. and allied markets as components; instead, they are part of a microelectronic system (which is predominantly assembled in Asia). In those cases, the amount of the subsidy on the chip is a very small percentage of the total value of the end product and thus not much of a deterrent. Other, more targeted, entity-based policies might be more effective in countering the threat of overreliance, but such discussions are beyond the scope of this paper. Suffice it to say that introducing a "trusted chip buyers alliance" to exclude countries of concern from allied markets broadly would face significant legal and practical hurdles, in addition to the abovementioned technical and commercial challenges of providing supply chain provenance.

[4] The antidumping and anti-subsidy provisions of the Tariff Act of 1930 allow for the imposition of tariffs based on threat, but it has been rarely used.

Policy Recommendations

Each of the above challenges must be addressed with specific policy solutions. Some, like secure MCUs, are specific to the semiconductor industry. Others, such as export controls or transparency and certification of supply chains, extend beyond semiconductors. It is beyond the scope of this paper to make recommendations for each of them. As it pertains to the discussion about "trusted" or "trustworthy" chips, this paper offers the following recommendations to policymakers:

- **Align on specific policy objectives rather than definitions.** Acknowledging that challenges, tools, and policy prerogatives may differ, aligning on clear, specific policy goals is important. A shared understanding is key to enabling problem-specific solutions. Often, the implementation will have to be country-specific, but integrated and aligned measures are needed to avoid negative spillover effects or loopholes. This is easier to achieve for discrete policy challenges than for a broad concept like "trusted chips."
- **Use, refine, and align existing policy tools devised for specific objectives.** Rules and tools already exist to address many of the current technical and geopolitical challenges facing the semiconductor industry. Policymakers should focus on jointly deploying these tools toward a common goal and augmenting national tool kits where there are gaps.
- **Enable and seek industry involvement to ensure commercial viability and promote fast adoption.** An innovative and competitive semiconductor ecosystem is essential for the United States and its allies. Implementing both "promote" and "protect" policies through regular exchanges with industry representatives is key. Moreover, industry compliance with those policies is crucial for their effectiveness. ■

***Andreas Schumacher** is a visiting technology fellow in the Economic Security and Technology Department and the Scholl Chair in International Business at the Center for Strategic and International Studies in Washington, D.C.*

*The author is grateful to **William A. Reinsch**, senior fellow and Scholl Chair in International Business, and **Barath Harithas**, senior fellow, Project on Trade and Technology, both at the Center for Strategic and International Studies, for valuable discussions and suggestions on this paper.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax- exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).