Detecting and Removing Counterfeit Semiconductors in the U.S. Supply Chain

The semiconductor industry seeks to partner with the government to address the threat of counterfeits entering the government supply chain. Recent media attention and government action has focused on potential security threats, but counterfeits are an immediate threat.

KEY FACTS

- Industry data has shown that <0.01% of legitimate semiconductor products will ever fail during operation in electronics systems.

- Counterfeit components are often "harvested" from electronics waste (e-waste) using crude processes then re-marked to indicate they are new or are otherwise different from how they were originally manufactured.

Risks of Counterfeits

The risks of counterfeit semiconductors are often misinterpreted and underestimated. Semiconductors are the "brains" inside critically-important electronic systems, including medical equipment, power grids, communications systems, automotive braking and airbag systems, and military and aerospace systems. When these critical components of our everyday lives contain counterfeits, they pose a unique risk to not only the health, safety, and security of consumers, but also to the economic prosperity of U.S. industry. However, much of the risk can be avoided.

Manufacturing and Reliability of Genuine Semiconductors vs. Counterfeits

The contrast between manufacturing of genuine semiconductors and counterfeit semiconductors could not be more extreme. Semiconductor companies spend tens of billions of dollars per year developing, manufacturing, testing, and supporting products that will operate to the highest quality and reliability levels for many years. Counterfeits are often "harvested" from electronic waste using crude and poorly-controlled processes that result in counterfeit semiconductors having far higher failure rates than genuine semiconductors. Some counterfeit semiconductors will fail immediately when electrically tested or first used, while others will fail after days, months, or years of field application. Counterfeit semiconductors jeopardize lives since they are prone to fail at the worst possible moments, such as when car airbags need to deploy, defibrillators are used to apply shocks, or when aircraft are landing.

Current Industry Initiatives to Combat Counterfeits

- Driving counterfeit component awareness and actions.
- Permitting Customs and Border Protection to work closely with manufacturers to keep counterfeit components from crossing borders and entering the critical supply chain.
- Partnering with law enforcement to help prosecute those involved in the manufacturing and/or trafficking of counterfeit semiconductor components.
- Evaluating component security features and developing international standards relating to supply chain assurance and anti-counterfeiting.

Require Government Purchase from Authorized Sources

- Government can significantly reduce the risks of counterfeit semiconductors from entering the supply chain by requiring purchase from authorized sources – original manufacturers and their authorized distributors.

- Products purchased through authorized sources are more cost effective in the long term, since they have superior quality and reliability levels, and carry full factory warranties.

- Any savings that DoD or their contract managers have realized by purchasing semiconductor components from the open market would be dwarfed by the costs of replacing previously-installed counterfeit components in fielded military systems.

- If semiconductors are not available from authorized sources, government should partner with industry to create a system to mitigate risks and purchase from alternative suppliers.

"Experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit. Overall, we estimate that counterfeiting costs US-based semiconductor companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs."

SIA President Brian Toohey
SASC Hearing
November, 2011