## Is There Cause For Concern?

**Consider these examples:**

- In 1999, The Cox Report was issued by the U.S. House of Representatives Select Committee on National Security and revealed that the People's Republic of China had stolen missile guidance technology used on missile systems for the Army and Navy, and on Navy and Air Force fighter jets.
- Between 2003-2005, eGlobe Solutions, based in Edmonds, Washington, sold nearly $1 million in counterfeit equipment to the Navy and Air Force.
- In 2008, Toshiba satellite laptops were shipped with the RavMonE.exe virus already installed; this virus allows unauthorized users to access information on a computer.
- In 2008, a European chip maker built into its microprocessors a "kill switch" that permitted remote access to the device in which these processors were installed; those with access could disable the microprocessor, making the item in which it was installed inoperable.

## How Can We Protect Against Threats?

The best way to protect microelectronics used for defense, national security and critical infrastructure systems is to employ a Trusted Supply chain that begins with design and fabrication in a facility accredited by the DoD Trusted Foundry Program. Using Trusted Suppliers mitigates the risk of tampering and provides assurance that the components will perform in the manner specified. Employing a Trusted supply chain allows a program manager to trust that the system will work as required, when required.

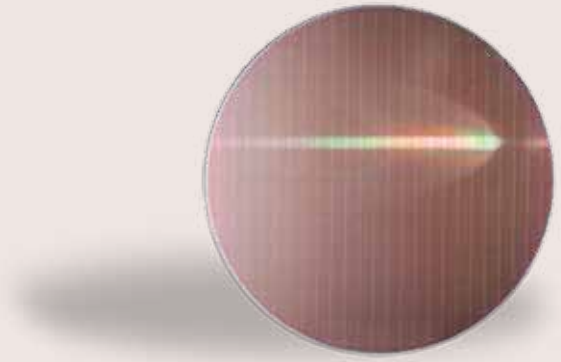
# Defense Microelectronics Threats: Real and Growing

- In 2011, the Pentagon revealed that a foreign government had launched a cyber-attack against military computers and stolen 24,000 files related to missile tracking systems, unmanned aerial vehicles, and the Joint Strike Fighter.
- In 2012, a California businessman was sentenced to prison for conspiring to sell counterfeit ICs bearing trademarks of legitimate semiconductor manufacturers.

**Detecting defects or unauthorized modifications in microelectronics components is difficult—sometimes impossible. The possibility for infiltration into, and malicious tampering with, DoD weapons and national security systems is real: a recent Department of Defense report revealed that DoD is hit with *10 million cyber attacks daily*. Building systems with Trusted microelectronics mitigates the hardware vulnerability aspect to cyber attacks, increasing the assurance that the United States can maintain its warfighting capability and preserve national security.**

http://www.dmea.osd.mil

TAPO
Trusted Access Program Office
https://www.tapoffice.org

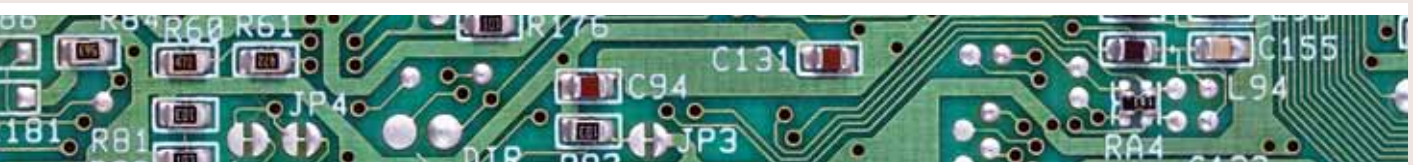


## *Trusted Foundry Program*

OSD R&E Defense Microelectronics Activity
NSA Trusted Access Program Office
https://dodtechspace.dtic.mil/groups/trusted-microelectronics

## Defense Microelectronics Threats: Real and Growing

During the past half-century, U.S. fighting forces have become increasingly reliant on individual equipment, weapons and communications systems, and command and control systems that incorporate microelectronics components. At the same time, the United States has gradually lost its dominant role in manufacturing these components. Today global business drives the microelectronics industry; defense requirements make up only a small part of the demand for Integrated circuits (ICs). Foreign manufacturers, most based in Asia, now supply ICs for both off-the-shelf end items and many of the systems designed specifically for defense.




In the past decade, U.S. defense, intelligence, and justice agencies have documented cases in which foreign suppliers and foreign governments have sought to make excessive profits, gain advantage over the United States tactically or strategically, or inflict damage on America's warfighting capability through the introduction of compromised microelectronics. When defective, these mission-critical components can render the most sophisticated equipment inoperable. The challenge the United States now faces in assuring the *integrity, security,* and *reliability* of microelectronics components employed in defense systems is a matter of national security. Hence, understanding the nature of the threat is vital to anyone working in the defense industry.

### What threats exist?

1 ***Counterfeiting:*** Manufacturers can fabricate, and suppliers provide, ICs that look like those specified to meet the demands placed on equipment in extreme conditions of combat and extended use. These inferior ICs can fail under stress and cause mission-critical components, end items, or systems to fail at moments when they are most needed.

2 ***Espionage:*** Manufacturers, sometimes at the prompting of foreign governments, can modify ICs to allow outside agents access once they are installed in end items. Modified ICs can make it easier for hostile agents to install malware (malicious software) that allows adversaries to gain valuable information about mission-critical systems.

3 ***Sabotage:*** ICs can be programmed to fail, making an end item inoperable. Similarly, ICs can be designed with components that allow unauthorized parties to access these chips. Malware loaded onto ICs before these components are delivered to DoD contractors or installed after a system is operational can be used to gain control of the weapon or communications device.

4 ***Supply Chain Disruption:*** Heavy reliance on foreign-made components and ICs places the United States at risk from businesses or governments that might refuse to fill orders for mission-critical materiel either for business or political reasons. In either case, this denial of service could make it impossible for America's fighting forces to obtain parts or end items required for defense.

### Where are the weak links?

Because most microelectronics are manufactured outside the United States, where quality standards may be inferior to those imposed in U.S. facilities, the greatest opportunity for malicious modification or counterfeiting occurs in fabrication plants. Facilities located in countries that see the United States as an adversary may find themselves encouraged to modify ICs so subversive activities may be carried out at a future date. Additionally, many firms that bid on contracts to supply DoD with components and end items sub-contract with third parties for manufacture and delivery of microelectronics. Sadly, some of these firms put profit over quality, substituting inferior parts which are marked as ones that meet DoD specifications. Mislabeling or mishandling ICs anywhere along the supply chain can lead to installation of components that do not meet specifications into important warfighting equipment. Using DoD accredited Trusted Suppliers for critical microelectronics provides protection against poorly manufactured or intentionally altered components, and gives greater assurance against supply chain disruptions.