Case Study: Defense Microelectronics Threats

Challenge: Because most microelectronics are manufactured outside the United States, where quality standards may be inferior to those imposed in United States 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.

Solution: 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.

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.

Defined Business Solutions

Connecting Innovation, Industry & Government

1701 Pennsylvania Avenue NW Suite 300
Washington DC 20006

www.definedbusiness.com

202-683-2021