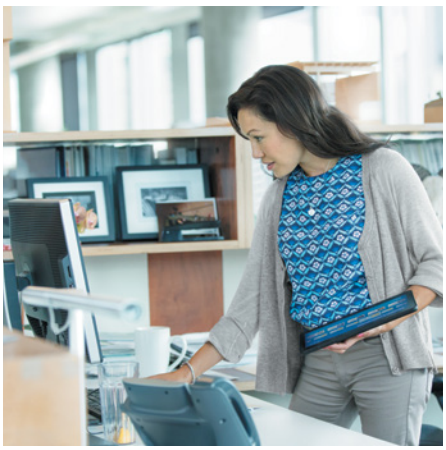
CASE STUDY

Transparent supply chain helps SGI

Introducing the transparent supply chain from Intel

How SGI is using the Intel® Transparent Supply Chain to meet US DFARS regulations



"We believe the Intel® Transparent Supply Chain implemented on our platform will enable us to meet the new DFARS 246.870-2 requirements by providing evidence that motherboard components were sourced from authorized dealers."

Cassio Conceicao, Chief Operating Officer, SGI

Emerging concern over counterfeit electronic parts

Since the mid-2000's, concerns have grown about how counterfeit electronic parts might cause safety hazards or failure of business critical applications. These concerns are described in the October 13, 2008 BusinessWeek cover story "Dangerous Fakes." A recent survey by Enterprise Strategy Group[1] reports that 16 percent of companies studied have purchased some form of counterfeit IT equipment. Current supply chain practices start with trusting the source, but processes are limited for screening out counterfeits, particularly for products containing many subsystems. As such, many companies may be unaware of counterfeit IT equipment infiltrating their datacenters. This is problematic on multiple levels – companies fund "bad actors" when they pay for counterfeits, and there is no way to ascertain reliability (mean time between failure) for counterfeits. This results in more downtime, higher support/maintenance costs and even safety concerns.

Like in many countries, the U.S. government is trying to close the holes. In 2011, U.S. Congress passed and President Obama signed into law new legislation requiring purchases controlled by Cost Accounting Standards (CAS) to "Detect and Avoid Counterfeit Electronic Parts." In 2015, the Defense Federal Acquisition Regulation Supplement (DFARS) extended these requirements beyond "CAS" contracts to include the small businesses set-asides.

SGI* partnered with Intel to address this issue

According to SGI* Chief Operating Officer Cassio Conceicao, "When it comes to counterfeiting, we don't know what we don't know, so a good first step is to start looking for methods that protect us even when we are unaware of any specific threat."

SGI selected the Intel transparent supply chain as a cost effective way to avoid counterfeits.

Requirements:

Prove that the electronic parts used in your products were sourced from either A, B, or C:

A. The original manufacturers of the parts;

B. Their authorized dealers; or

C. Suppliers that obtain such parts exclusively from A or B.

SGI believes using the Intel transparent supply chain meets these requirements

According to SGI Chief Operating Officer Cassio Conceicao, "We believe the Intel transparent supply chain implemented on our platform will enable us to meet the new DFARS 246.870-2 requirements by providing evidence that motherboard components were sourced from authorized dealers.

Our customers want to know that their hardware is coming from a credible manufacturer and that the manufacturer can provide a high level of authentication. The Intel transparent supply chain provides a digitally sided certificate bound to each server they supply.

Transparency enables SGI to sell an appliance that can be traced at a component level through its entire supply chain to a credible hardware root of trust.

Transparency enables "trust but verify"

Intel's strategy is aligned with ISO/IEC supply chain guidelines 20243 and 27036. Intel factories have processes and procedures that track sources for critical components placed on each server board.

The benefit of transparency is:

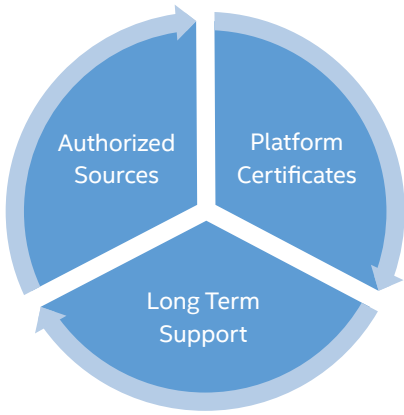
1. Evidence that critical components and firmware came from authorized sources.

2. Features designed to authenticate that a particular platform was manufactured by Intel's authorized partners.

3. Provenance statements are anchored to a hardware root of trust[2].

Security is important to any business. SGI, with Intel's help, is leading the industry to drive a higher level of trust in their supply chain. Critical infrastructure organizations and governments want to verify they can trust and are protected against counterfeit part threats.

Find the solution that's right for your organization. View **success stories from your peers** and check out the **IT Center**, Intel's resource for the IT Industry.



[1] http://www.esg-global.com/research-reports/cyber-supply-chain-security-revisited/

[2] See https://en.wikipedia.org/wiki/Trusted_Platform_Module

1215/MS/JS/CC/PDF

333711-001US