

Study: Fake Military Parts on the Rise
By: Jen DiMascio
February 16, 2010 05:14 AM EST

Already heavily taxed by two wars and repeated worldwide deployments, the U.S. military is facing yet another challenge: the increasing intrusion of counterfeit electronics and other parts into its supply lines.

And a new Commerce Department study finds the Pentagon is barely addressing the problem.

The study of contractors, subcontractors and Defense Department agencies tracked the rise in counterfeit electronics entering the system since 2005 – from 3,868 incidents then to 9,356 in 2008. The Navy's Air Systems Command asked for the study, suspecting that many more counterfeit and defective electronics were finding their way into the Pentagon's vast supply chain in ways that could affect the reliability of weapons.

The study found many flaws within the system: The different organizations, contractors, subcontractors, manufacturers, distributors and agencies themselves don't talk enough about the issue. There's a lack of accountability within organizations. Recordkeeping about instances of counterfeit parts is limited. And most organizations don't know whom to contact in the government when confronted with fakes.

Most Pentagon organizations, the report also found, don't have policies in place to thwart counterfeit parts.

Industry is aware of the trend, too, with Boeing's high-tech division Phantom Works briefing at conferences on ways to avoid counterfeits.

One industry official said the problem isn't limited to electronics. Foreign suppliers using substandard materials could be producing rivets, bolts and screws that hold together everything from missile casings to ship ladders.

"If we make it, they can fake it," the official said.

The explosion of counterfeit parts is being driven by an expanding global economy and an emphasis on low-price contracting – both of which come as the Pentagon is relying more heavily on older platforms, with parts that are becoming obsolete.

And it's all being exacerbated, the Commerce Department study found, by weaknesses in a system that's supposed to catch the flaws.

"There is an assumption that others in the supply chain are testing parts. Organizations within every sector rely on others in the supply chain to test and verify the authenticity of parts and, therefore, conduct little testing themselves," the report said. "Based on survey data, this confidence in the testing behaviors of the supply chain is unfounded."

It's a problem that affects the entire federal government.

Any business has an equal opportunity to sign up as a vendor with the General Services Administration, said Ram Manchi, president of the Alliance for Gray Market and Counterfeit Abatement. And once a business is added to the GSA list, government agencies can start buying goods from it.

It's more difficult to gain approval to sell goods such as electronics, information technology and software. But once vendors are in the system, controls are so lax that they have flexibility to sell almost anything to any agency.

"One can register for selling Scotch tape and sell network routers," Manchi said. "Where the lowest-price bid drives the purchasing decision, the GSA process fails to keep out the fraudsters and criminals and exposes agencies to sources of substandard goods, including counterfeits."

Vice Adm. Alan Thompson, who leads the Defense Logistics Agency, which is in charge of the Pentagon's vast inventories of almost 5 million items, readily acknowledges the problem.

"It's something that frankly concerns me," Thompson told reporters recently. "We have to be on our toes." As a result, Thompson said, his agency has instituted "very aggressive" efforts to snare fraudulent parts. And despite the findings of the Commerce Department, Pentagon officials say the Defense Department does check to make sure fakes don't slip through the cracks.

"We continue to assess our processes to mitigate the risk of counterfeit parts. Various studies and tests have occurred to address this issue," Pentagon spokeswoman Lt. Cmdr. Wendy Snyder told POLITICO.

"When these studies and tests have identified incidents of counterfeit parts, those parts are extracted from the system, documented, analyzed, and the appropriate actions are taken quickly," she said. "The department has not found any cases where counterfeit parts have caused failure of DoD missions, equipment or placed our troops at risk."

And she noted that the Defense Logistics Agency has a series of checks and balances to stymie the flow of counterfeits – buying from a list of qualified suppliers, pushing for documentation, testing samples and litigating when counterfeits are discovered.

One such case has been in federal court in Washington.

Three Californians – Neil Felahy, his wife, Marwah Felahy, and his brother-in-law Mustafa Abdul Aljaff – were charged with trafficking in counterfeit goods. Neil Felahy pleaded guilty last November and agreed to cooperate with the government on the condition that charges against his wife be dropped, according to news reports. Aljaff pleaded guilty last month. Sentencing for both men is pending.

Over a two-year period, the trio set up a number of companies – including MVP Micro, Labra Electronics and Red Hat Distributors – that ferried \$140,835 worth of counterfeit circuits from Shenzhen, China, to

the United States, marked with familiar brand names: Fujitsu, Atmel, Intel and Altera.

To pass them off as brand-name parts, the companies used semiconductor-grade acetone or melted plastic casings to remove original labels and rebranded them to meet military grade, according to the court proceedings.

Last spring, the court documents said, the three scored a contract with the Navy for the sale of integrated circuits, complete with a Certificate of Conformance, required by the Pentagon: "It is hereby certified that all materials shipped on our purchase order conform to the applicable military and/or commercial specifications."