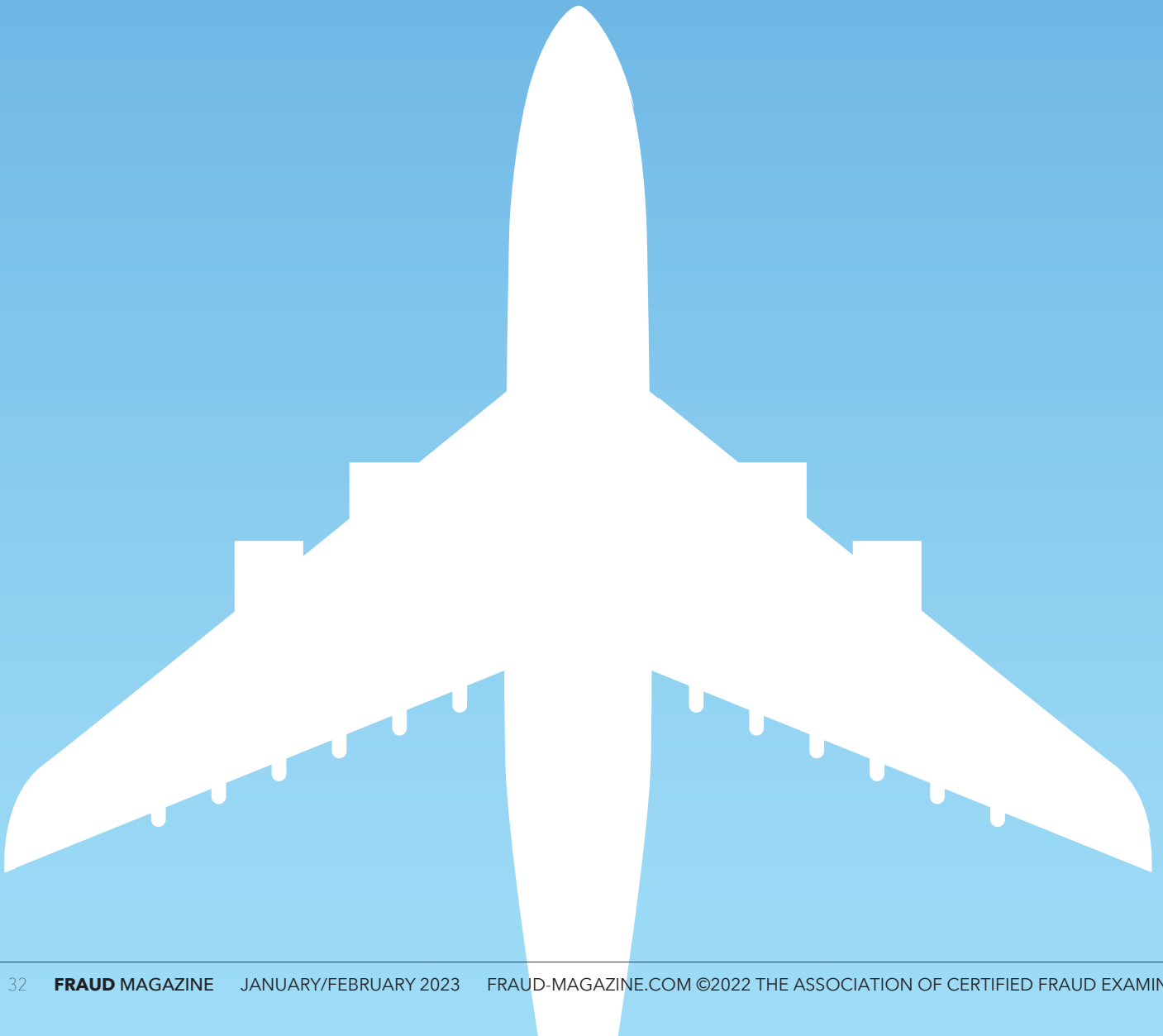




BATTLING **fraudulent product** **substitution**

By Stewart Thompson, CFE





Fraud fighters have long been aware of the dangers of product substitution and counterfeit parts in military equipment. But global supply chain shortages and the U.S. armed forces' need for obsolete parts have exacerbated the problem. Here a former NCIS agent talks about his experience and how a more proactive approach can help.



Imagine for a minute that you're an Air Force pilot flying the fighter jet F-16CM Falcon and you're returning to base after a nighttime training mission. While attempting to touch down on the runway, you discover that your landing gear is damaged. You execute a go-around and try to land again, this time by having the plane's tailhook catch an arresting cable. That fails too, and the wing touches the runway. As the plane starts to crash, you reach down and pull the ejection handle, which releases the canopy. An explosive cartridge launches your seat over a hundred feet into the air. But your parachute fails to deploy, and you realize you're about to slam into the ground, still strapped into your seat, with only a fraction of a second to go before your death. How could a scenario like this happen? Once an ejection handle is pulled, it triggers an almost instantaneous sequence of events aimed at getting the pilot safely to the ground. But in this real-life example of the potential dangers of product substitution, an Air Force investigation later revealed that the failure of the seat's digital recovery sequencer (DRS) — which

controls the timing of the ejection — contributed to the pilot's death. Not only that, but the electronic components inside the sequencer were reportedly counterfeit, even though the F-16 manufacturer maintained the strictest quality controls over its subcontractors that built the ejection seat and the DRS.

This incident is based on the true story of First Lt. David Schmitz, an F-16 Fighting Falcon pilot, who died in June 2020 in a botched landing after his ejection seat failed to deploy its parachute. It underscores the need for strict enforcement of U.S. Department of Defense (DOD) standards for military parts. And an important part of that is the aggressive investigation of anyone suspected of prioritizing profits over safety by substituting subpar components to meet contract demands and passing them off as parts that meet the standards. (See "An F-16 pilot died when his ejection seat failed. Was it counterfeit?" by Rachel S. Cohen, Air Force Times, Sept. 13, 2022, tinyurl.com/5n9amjba.)

Because of the enormous amount of government funding that goes into the defense sector, the U.S. military has long suffered its fair share of fraud. And

counterfeit components/product substitution — which is really a category of procurement fraud all on its own — remains an ongoing problem.

With the U.S. government looking to replenish billions of dollars in military aid to Ukraine on the back of supply chain woes, fraud fighters are once again on high alert for signs of fraud and abuse. In fact, there are even more pressures and opportunities to commit this type of fraud, as people seek illicit sources for parts amid a global supply chain crisis that has created a rich environment for fraud and made the U.S. more vulnerable to threats from foreign adversaries.

Concerns about the use of Chinese components in U.S. military equipment are on the rise not only because they might be counterfeit but also for their potential use in sabotage and spying as military and economic competition between the two superpowers intensifies. Earlier this year, FBI Director Christopher Wray warned that the Chinese government "poses the biggest long-term threat" to the economic and national security of the U.S. and its allies. (See "Heads of MI5, FBI give joint warning of growing threat from China,"

by Juby Babu, Reuters, updated July 7, 2022, tinyurl.com/yw9prmk.)

Just last September, the Pentagon and Lockheed Martin suspended deliveries of F-35 fighter jets after discovering that a subcontractor had used a magnet made of cobalt and samarium alloy that came from China. Lockheed described the supplier of the alloy as a “fifth-tier” supplier amid concerns that the Chinese-sourced materials might have violated the Defense Federal Acquisition Regulation Supplement — requirements and regulations designed to maintain the integrity of sensitive government information that third parties might hold or use. [See “Pentagon suspends F-35 deliveries over Chinese alloy in magnet,” by Stephen Losey, Defense News, Air Warfare, Sept. 7, 2022, tinyurl.com/yydbz6fx and “Defense Federal Acquisition Regulation Supplement (DFARS),” Security Encyclopedia, tinyurl.com/4m9we9m9.]

As a retired special agent for the Naval Criminal Investigative Service (NCIS), I spent many years investigating product substitution cases for the Navy. Here I look back on how the NCIS took a renewed interest in counterfeit parts, the latest cases of wrongdoing in this corner of the fraud world and how NCIS’s proactive approach can make all the difference in detecting and preventing product substitution.

A renewed focus on product substitution

After the 2000 USS Cole bombing and the Sept. 11 terrorist attacks in 2001, the NCIS’s fraud program was overshadowed by those events and became extinct ... almost. The NCIS resurrected it, largely due to the efforts of former Special Agent Louis Lockwood, who in 2005 became NCIS’s division chief, economic crimes, which is the department responsible for safeguarding the Navy’s acquisition programs from fraud and corruption. Lockwood developed and implemented the Integrated Agent Fraud

Program at major U.S. Navy commands to supplement its more traditional, reactive role. He also helped procure funding so that NCIS agents could obtain their CFE credential, realizing they needed the training the ACFE offers. [See “I’m a CFE - Nancy Rich, CFE, Special Agent at the Naval Criminal Investigative Service (NCIS),” by Emily Primeaux, *Fraud Magazine*, September/October 2014 issue, tinyurl.com/2xxbhcvw.]

Lockwood envisioned that agents would embed themselves in major Navy command headquarters to develop close relationships and promote fraud awareness through briefings. This proactive approach would help agents better understand and assess command vulnerabilities and concerns. It was during this time that Admiral Walter Massenburg took over the reins as Commander of Naval Air (NAVAIR) Systems Command in Patuxent River, Maryland.

In 2005, members of the NCIS Economic Crimes Division, Washington, D.C., went down to NAVAIR to brief Massenburg on the Integrated Agent Program. Debbie Winslow, NCIS assistant special agent-in-charge, told me that when Massenburg was asked to identify his major concern, he replied, “What keeps me up at night are potential safety mishaps involving our aircraft.”

That philosophy continues to this day as NCIS works alongside other government agencies to prevent this type of fraud and the accidents it causes. Here are some recent cases of product substitution, involving NCIS and the Defense Criminal Investigative Service (DCIS) — the investigative arm of the Office of Inspector General, U.S. Department of Defense (DOD). (See “Semi-annual Report to the Congress,” Inspector General, DOD, Oct. 1, 2021, through March 31, 2022, tinyurl.com/4mkww6h3.)

- In February 2022, Elaine Thomas, the former director of metallurgy at Bradken Inc., was sentenced to 30 months

in prison and fined \$50,000 after years of falsifying the results of tests to measure the strength and toughness of steel used in Navy submarines. Bradken is the Navy’s leading supplier of high-yield steel castings for submarines, which can’t fail during a collision. But for 30 years, Thomas falsified test results to hide that its castings failed to meet the Navy’s rigorous standards. Bradken agreed to pay a nearly \$11 million civil settlement related to the case. In all, the fraud affected 30 submarines, and the Navy has had to spend nearly \$14 million to assess the risks to the vessels.

- From 2012 to 2019, Brighton Cromwell, LLC, a military vehicle parts supplier, allegedly provided the DOD with non-conforming materials and knowingly violated the Defense Federal Acquisition Regulation Supplement by selling items without determining whether they were manufactured according to the Buy American Act or the Trade Agreements Act. Brighton Cromwell also allegedly breached its contracts with the government after selling it items manufactured or assembled in prohibited countries. In 2021, it agreed to pay \$850,000 to resolve these allegations.

Dangers lurking in the gray market

Historically, the DOD has relied on companies like Bradken and Brighton Cromwell to manufacture or sell parts for military aircraft and weapon system applications. However, as the cases above illustrate, unscrupulous companies have used various methods to introduce counterfeit or non-conforming parts into the DOD procurement chain. This is worrisome because counterfeit parts imported from abroad and sold to DOD distributors can potentially compromise U.S. national security.



Because of the enormous amount of government funding that goes into the defense sector, the U.S. military has long suffered its fair share of fraud. And counterfeit components/product substitution – which is really a category of procurement fraud all on its own – remains an ongoing problem.

These items can contain malicious computer code and create a back door into DOD networks, enabling a foreign adversary to access sensitive information to commit espionage. And the gray markets — where items are sold outside the manufacturer's authorized channels — have been a particular concern. (See "Brand Protection Insights from Industry Leaders in Gray Market, Counterfeit and IP Fraud Mitigation," by Sherri Erickson, De La Rue and John Solheim, FiveBy Solutions, December 2020, tinyurl.com/4b6zade8.)

Gray markets aren't new. Nor is their use to game the U.S. military procurement system. In 2006, a U.S. district court charged the owners of eGlobe Solutions Inc, an authorized seller of Cisco Systems products, with defrauding the government on computer equipment contracts worth \$788,000. They allegedly sold gray-market and counterfeit products from China to the Navy. Unauthorized vendors also altered that equipment to appear as if the product met the contract specifications. (See "Edmonds Brothers Charged With Defrauding The Government on Computer Equipment Contracts," DOJ, press release, Nov. 16, 2006, tinyurl.com/4rs9npu4 and "Inspector General United States Department of Defense Semiannual Report to the Congress, Oct. 1, 2006 – March 31, 2007," tinyurl.com/m9kewsyp.)

Against this backdrop, major prime contractors at NAVAIR were reporting in the Government-Industry Data Exchange Programs (GIDEP) increasing procurements of counterfeit integrated circuits (ICs) from multiple independent distributors. (See "Counterfeit Part Reporting Trends," by Henry Livingston, Feb. 11, 2014, tinyurl.com/4fw23bf6.) GIDEP is an information-sharing program between the U.S. government and industry. GIDEP's database receives and disseminates information about nonconforming products and materials. The DOD has also designated GIDEP as its central database on obsolete military parts and those parts with a diminishing number of manufacturers. (See www.gidep.org.)

Clamping down on counterfeit parts

By the early 2000s, the rise in this type of fraud helped spur a series of investigations by law enforcement into the distribution of counterfeit network hardware, bringing together various agencies including the NCIS and DCIS. (See "Departments of Justice and Homeland Security Announce International Initiative Against Traffickers in Counterfeit Network Hardware," DOJ, Feb. 28, 2008, tinyurl.com/wtv6wzsh.)

In the case that laid the foundation for the creation of the largest task force

investigating counterfeit parts — Operation Chain Reaction — Stephanie A. McCloskey was sent to prison in 2011 for importing counterfeit integrated circuits from China and Hong Kong and selling them to the U.S. Navy and defense contractors. McCloskey and others had run their operation from a Florida-based firm called VisionTech Components, generating \$15.8 million from those sales. I was the case agent at NCIS, which conducted the investigation jointly with U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI). (See "VisionTech administrator sentenced to prison for role in sales of counterfeit circuits destined to US military," U.S. Department of Homeland Security, Oct. 25, 2011, tinyurl.com/ytbehkhf.)

BAE Systems Electronic Solutions had reported that it and NAVAIR had jointly procured suspected counterfeit microcircuits from a parts broker; this broker had purchased the discrepant devices from a second tiered subcontractor based in Florida, which we now know was VisionTech. NAVAIR and BAE had procured these parts for the purpose of installing them in ship and land-based antenna equipment related to the identification friend foe (IFF) system, which enables the military to identify whether incoming aircraft or vehicles are friendly or hostile.

In a related case I worked on, owners of California-based company MVP Micro were sentenced to 20 months in prison for importing counterfeit microchips from China. In a process called “blacktopping,” the owners took legitimate chips, sanded off the brand markings and re-marked them to make them appear to be of a higher quality. The company owner was indicted and pleaded guilty in U.S. District Court. One of the counts he pleaded to was purchasing a counterfeit, military-grade integrated circuit from VisionTech. (See “Three California Family Members Indicted in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military,” DOJ, Oct. 9, 2009, [tinyurl.com/yc2ja2dx](https://www.tinyurl.com/yc2ja2dx) and “Operations Manager for MVP Micro Sentenced to 20 Months in Prison For Conspiring to Sell Counterfeit Microelectronics to the U.S. Military,” DOJ, Feb. 22, 2012, [tinyurl.com/mry4e869](https://www.tinyurl.com/mry4e869).)

Other investigations involved different agencies, including the Federal Aviation Administration (FAA), NASA Office of Inspector General (OIG), and the U.S. Department of Transportation OIG, as both civilian and military aircraft share many of the same parts. For example, one company, which had contracts with NAVAIR and NASA, altered test results and falsified

Unscrupulous companies have used various methods to introduce counterfeit or nonconforming parts into the DOD procurement chain. This is worrisome because counterfeit parts imported from abroad and sold to DOD distributors can potentially compromise U.S. national security.

certificates of conformance (CoCs) for parts destined for use in the space shuttle. An authorized party typically provides a CoC to verify that a product meets certain standards of specification. (See “What is a Certificate of Conformance?” My Accounting Course, [tinyurl.com/yvb9vdx](https://www.tinyurl.com/yvb9vdx).) This resulted in the FAA issuing an unapproved parts notification (UPN), initiating a suspected unapproved parts (SUP) investigation and sharing the information with law enforcement agencies. (See “Owners of Florida Aerospace Metals Supplier Pleads Guilty to Supplying Customers with \$854,379 in Sub-Standard Metals,” OIG, U.S. Department of Transportation, Sept. 12, 2006, [tinyurl.com/2drxcyw9](https://www.tinyurl.com/2drxcyw9).)

As part of these cases, we reviewed U.S. Customs and Border Protection (CBP) import/export seizure records with the assistance of Homeland Security’s Intellectual Property Rights Resource Center and found that the implicated companies distributed counterfeit electronic components and violated U.S. export licensing requirements. As a result, the original equipment manufacturers would often issue cease-and-desist letters to the contractors receiving the bogus parts to protect their brands against trademark infringement. I shared with NCIS’s Foreign

Counterintelligence Division all intelligence gleaned from companies abroad that were importing counterfeit parts into the U.S.

Despite efforts to put an end to this type of fraud, law enforcement and manufacturers continue to fret about the sale of unauthorized parts through the gray market and other means. Cisco Systems recently warned that the disruptions in the global supply chains due to the pandemic have encouraged its customers to turn to unauthorized channels to purchase its gear. This has resulted in a spike of availability of counterfeit/gray-market Cisco equipment. (See “Cisco Warns Supply Chain Issues Causing Spike In Gray Market, Counterfeit IT Gear,” by Gina Narcisi, CRN, Networking News, April 28, 2022, [tinyurl.com/53xu69d8](https://www.tinyurl.com/53xu69d8).)

Need for obsolete parts

Many micro components installed in military and aerospace applications are tested to withstand conditions typically experienced in a military environment such as shock, vibration, salt spray, high-altitude pressures and extreme temperature ranges. As a result, many of these parts are labeled as military grade. Fake components could work perfectly fine for months and

then prematurely fail when most needed long after installation and use.

The problem is exacerbated by the fact that the DOD relies on obsolete parts, especially brand-name, trademark-protected microchips, to maintain its aging aircraft fleet and weapon systems. DOD aircraft and other weapon systems are designed to operate with upgrades for decades. In many cases, original equipment or component manufacturers no longer make or upgrade the proprietary semiconductors used in the systems, because it's no longer cost-effective. This forces the DOD to turn to outside channels, such as unauthorized distributors or parts brokers, which leaves the industry vulnerable to procuring counterfeit or gray-market materials. In addition, global supply chain disruptions create even more of an opportunity for brokers to sell fake parts. (See "Fraud's fertile breeding ground," by Stephen Pedneault, CFE, CPA/CFF, *Fraud Magazine*, January/February 2022 issue, tinyurl.com/4cn4j8n9 and "Chip shortages result in record wire fraud reports by desperate buyers," by Jane

Lanhee Lee, Reuters, June 28, 2022, tinyurl.com/2p8zm38x.) It's hoped that the recent passage of the U.S. CHIPS Act bill will boost the production of microchips in the semiconductor industry and help alleviate these shortages. (See "The proposed legislation to boost semiconductor manufacturing," by Alex McLendon, WDET, July 23, 2022, tinyurl.com/yrmsukeu.)

Understanding the vetting process

Before examining proactive methods implemented at NAVAIR, it first may help to understand the vetting process for supply contracts in the U.S. armed forces.

The Defense Contract Management Agency (DCMA), which administers contracts for the DOD, carries out a process known as origin inspection and acceptance. This involves going to the contractor's facility to inspect and verify the product for acceptance. The DCMA works directly with the defense contractor to ensure sufficient technical systems are in place to produce the products and

that products presented for acceptance satisfy established contract technical requirements.

Alternatively, a contract may simply stipulate destination acceptance. This means that the organization where the product was sent will administer the inspection and acceptance process for the government. As part of DCMA procedures, it's common to have DOD employees, known as quality assurance representatives (QARs), perform on-site inspections to confirm that quality procedures are in place and to perform material acceptance inspections. In addition, DCMA QARS witness various types of testing to verify that contractual requirements are met.

When the DOD identifies a standard part, the supplier typically claims innocent error or that the government reported the deficiency long after the expiration of any warranty. This usually results in either a credit to the government or some determination of cause or blame. When the DOD detects nonconforming parts, it's often difficult to prove intent to



defraud without compelling evidence. The DOD normally administers each problem as a separate instance and rarely conducts an analysis of the overall practices of the vendor for possible referral for criminal investigation. Law enforcement agencies have traditionally investigated bogus parts cases reactively. This investigative approach of addressing the problem and of developing and prosecuting bogus parts cases has had only limited success.

Proactive prevention

A proactive approach provides a more effective and efficient means of obtaining evidence to prosecute suspects, who are predisposed to supplying nonconforming parts to the DOD. This starts with monitoring suppliers for red flags. A disproportionate percentage of deficiency reports, failed tests or inspections, and terminations for convenience or default are good indicators of chronically unreliable suppliers, whether they're careless, unscrupulous or possibly both.

Here's one case that underscores the importance of paying attention to these warning signs. In 2006, the DCIS and NCIS initiated an investigation, implicating the owner of four companies in knowingly providing nonconforming parts to NAVAIR. For example, the companies failed to conduct contractually required testing and falsified CoCs.

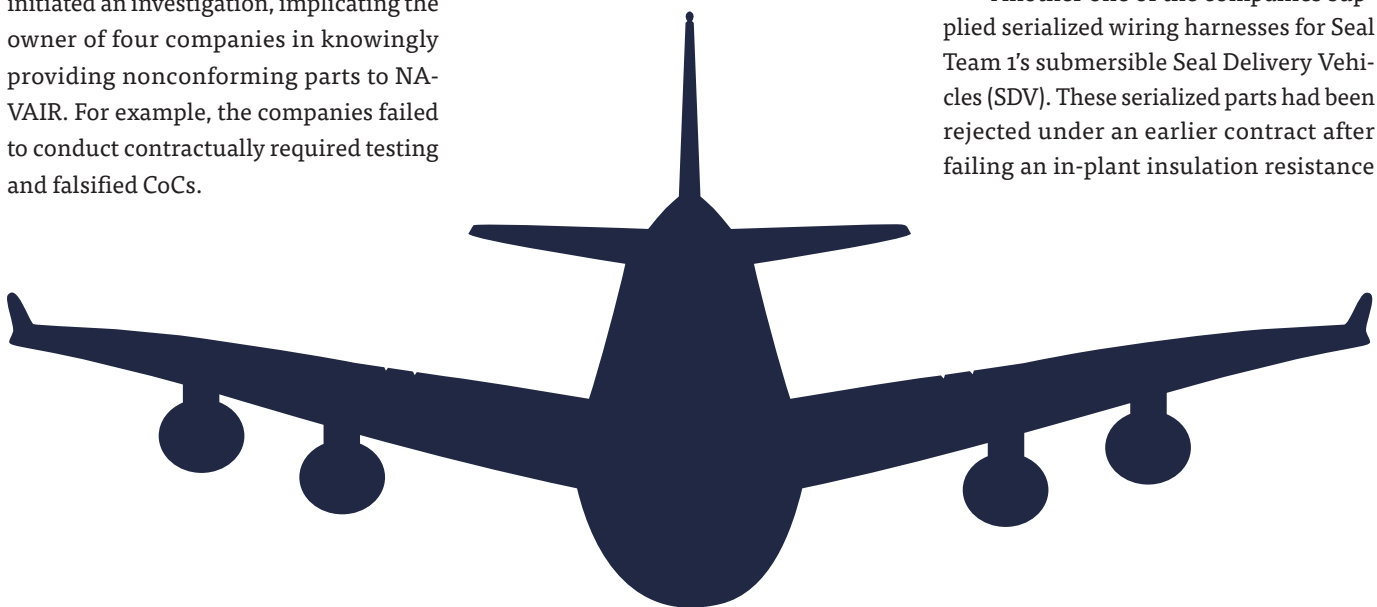
A review of the pertinent DCMA file and witness interviews revealed the QARs had issued these companies numerous corrective action requests (CARs), documenting the contractors' quality deficiencies, including repeated testing failures. CARs provide written notification to a contractor that the parts inspected were rejected and inform the contractor of the reason for the failure. These companies also had a lengthy history of failing first article testing (FAT) inspections witnessed by QARs or independently performed by NAVAIR engineers to ensure a contractor can correctly make the part.

The investigation revealed that one of the companies failed a FAT inspection for a motor cable, part of the weapons system for a U.S. Marine Corps amphibious vehicle. The cable was classified as a critical application item (CAI), meaning if it failed it would likely impact the ability or performance of a weapon system to carry out a required mission. After the testing failure, the contract was terminated for default. Despite that the company subsequently provided motor cable assemblies with the same part number, including a CoC, under a destination acceptance DOD contract.

Queries of product quality deficiency reports (PQDRs) revealed that the companies provided nonconforming parts to the DOD. PQDRs are part of the Navy's product data reporting and evaluation program (PDREP), which is useful in locating companies selling nonconforming products/services to the government. (See tinyurl.com/z92n83a3.)

For example, one of the companies involved in this case was issued a PQDR after supplying defective cables associated with the AIM-9 missile's guidance system. The cable was classified as a CAI. The PQDR concluded that the parts didn't pass calibration tests. Had they been installed, the missile system would've likely been rendered inoperable. The AIM-9 (Sidewinder) is a supersonic heat-seeking missile carried by U.S. fighter aircraft. This is an especially effective weapon as the pilot can fire the missile and immediately exit the area to get out of harm's way. The DCMA had previously rejected the parts after they failed in-house testing, resulting in the issuance of a CAR. But the contractor then sold the parts, accompanied by a CoC, to a commercial distributor, which in turn, sold them to the DOD.

Another one of the companies supplied serialized wiring harnesses for Seal Team 1's submersible Seal Delivery Vehicles (SDV). These serialized parts had been rejected under an earlier contract after failing an in-plant insulation resistance



“What keeps me up at night are potential safety mishaps involving our aircraft.”
- Admiral Walter Massenburg

test, which resulted in moisture entering the cable/connectors. After receiving the parts, Seal Team 1 authored a PQDR. One part bore the same serial number as the one that the DCMA QAR had previously rejected. Had these parts been installed, a failure would've had potentially disastrous consequences to the safety of the crew during high-risk exercises and missions, as the vehicle would need to surface. (See "Indictment alleges business owner defrauded U.S. gov't.," *Centraljersey.com*, Aug. 13, 2008, tinyurl.com/bdfthedh and "Monmouth County Defense Contractor Pleads Guilty to Making False Statements to Defense Department," DOJ, Jan. 15, 2010, tinyurl.com/zuvmaxnb.)

Working together

NAVAIR carried out proactive operations to help determine whether suspects knowingly provided nonconforming parts for use in military systems. To make these determinations, NCIS/NAVAIR would fund the purchase of parts from subject contractors. Law enforcement agents worked with NAVAIR to conduct research relating to the military specifications associated with the parts. The relevant military command or agency — i.e., NAVAIR, DCMA, or Naval Sea Systems Command — provided the specifications, which would, in turn, be given to the suspected supplier. Once NCIS received the parts, they were entered into

evidence. The parts were then tested for compliance with contract specifications by NAVAIR's system engineering department or the original manufacturer of the part, which was often a member of the Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force (ACTF). The SIA ACTF provided direct support to law enforcement in the form of reporting suspected counterfeit devices and in testing suspected counterfeit parts. (See "Anti-Counterfeiting," SIA, tinyurl.com/6ju5ve9k.)

If the parts failed testing, then law enforcement agents considered making repeat buys. Sources engaged subjects in consensually monitored telephone conversations to potentially elicit incriminating statements and to request any test data from the company and CoCs that the supplier hadn't already provided. NAVAIR would identify all platforms in which the discrepant parts were installed. NCIS would notify sister law enforcement agencies if their organizations were impacted. Law enforcement agents worked closely with the relevant assistant U.S. attorneys to apply for and execute search warrants. After the criminal case was completed, it was referred to the pertinent debarment



activity for civil remedies to initiate debarment and suspension proceedings.

The above examples demonstrate how some contractors and parts distributors egregiously supply nonconforming parts to the DOD despite the best efforts of government to prevent this type of fraud. Bad actors can still find ways to intentionally sell defective goods through distributors that knowingly or innocently sell bad parts to the DOD or to major contractors. This underscores the importance of implementing proactive operations at various military commands to combat product substitution. ■ **FM**

Stewart Thompson, CFE, is a retired special agent for the Naval Criminal Investigative Service (NCIS). He served over 25 years at the U.S. Department of Defense and as an insurance fraud investigator with the State of Maryland. Contact him at thomps4649@gmail.com.