Lieutenant General Patrick J. O'Reilly, USA
Director, Missile Defense Agency
Before the
Senate Armed Services Committee
November 8, 2011

Good morning, Chairman Levin, Ranking Member McCain, other distinguished Members of the committee. I appreciate the opportunity to testify before you today on the problem of counterfeit electronic parts infiltrating our critical defense systems and the steps the Missile Defense Agency (MDA) is taking to detect and prevent unauthorized or defective parts from being integrated into the Ballistic Missile Defense System (BMDS).

MDA integrates technologically advanced sensor, fire control, battle management, and interceptor systems into a single BMDS to provide a reliable, continuously available, defense of our homeland, deployed forces, allies, and friends against a variety of regional ballistic missiles. The BMDS is one of the most complex systems being developed in the Department of Defense (DoD), and the reliability of the BMDS is only as good as the least reliable component of an interceptor, or any vital sub-system.

There are more than 3,000 suppliers providing parts, materials, subassemblies and assemblies for the BMDS. Each one of our missile defense interceptors comprises hundreds of assemblies containing items such as circuit boards, wire harnesses, connectors, valves, solid rocket motors, and electro-mechanical motors. There are also imagery systems, electro-explosive devices, optical devices and precision inertial components. Each assembly has a specific function to fulfill at specific times and it must perform in harsh environments and stressful conditions. We expect the piece parts of these assemblies to perform flawlessly when needed.

Throughout the development process, we carefully scrutinize the designs to make sure design margins exist. We manage the build process to ensure product manufacturing repeatability. Prior to fielding such systems, we test each assembly under stressful environments, thus assuring ourselves and the American people that the systems we employ will perform as required. A simple change in material, an improper technique in material application, or a lack of cleanliness during manufacturing can result in a loss of quality and, hence, a loss of system reliability.

DoD contractors primarily obtain parts from Original Equipment Manufacturers (OEMs) or from distributors the OEMs authorize. An Unauthorized Distributor is one who is not licensed by the OEM to sell its product. We view a counterfeit part as a part procured from an Unauthorized Distributor that is a copy or substitute assembled or sold without the OEM's permission or authority to do so; or one whose material, performance, or characteristics are misrepresented by a supplier in the supply chain. Whether the part was knowingly misrepresented has little programmatic consequence to the execution of MDA programs, we still have to deal with an unanticipated parts replacement challenge.

One type of counterfeit part is a used part that is re-marked, has an unknown pedigree and, when sold as new, has most likely been exposed to extreme environments such as high temperature necessary to remove the part from a Printed Wiring Board. Delamination of the internal die bonding can occur as a result of the thermal shock from the heat source used to remove the part from a used circuit board. These unknown conditions expose the part to potential failure modes that could be manifested after acceptance testing. Additionally, exposure levels to humidity and

electro-static discharge are unknown. The mechanical parameters of the part may also be changed. Lead wire integrity may be impacted during the removal and remanufacturing operations. Hermetically sealed military parts may get cracked during removal, exposing them to humidity and corrosion that would not appear during acceptance testing but could appear as a failure in the field.

Parts can be re-marked as being a fully military compliant part when in fact the part may only be a commercial version of the part. Later revisions of a part may operate in a slightly different manner than previous versions of the part (one or more performance specs may have been tightened over time). If the circuit application requires a newer part, a previous version remarked as a later version may cause latent failures. Because counterfeiting continually evolves in sophistication, it is possible that electronic parts may have embedded functionality created by an enemy seeking to disable a system or obtain critical information. Detecting hidden functionality would be a difficult undertaking.

MDA has encountered incidents of counterfeit parts dating back to 2006. We identified seven incidents (6 assemblies) of counterfeit parts. Part-level testing, acceptance testing, stockroom sweeps and an identification of parts bought by Unauthorized Distributors helped surface these instances. In one counterfeit part incident, a single acceptance test failure prompted further investigation into the pedigree of the part that failed. The subsequent investigation found that over 1,700 read-only memory parts were procured from an Unauthorized Distributor and had questionable attributes, such as multiple lot date codes and indications that the parts were previously used. This case resulted in removal and replacement of almost 800 parts from

assembled hardware. In another system, a non-mission critical system, electrical testing during acceptance testing yielded erroneous functionality from a voltage regulator. Further investigations showed that the parts were procured from an Unauthorized Distributor and had external markings that were not in accordance with the part drawing. Further investigations found variations of the internal part die. As a result, 38 assemblies were reworked and 250 parts were discarded. In another mission critical system, two acceptance testing failures prompted failure investigations that resulted in the identification of a counterfeit operational amplifier. In this case, 20 assemblies and 150 parts were impacted. A stockroom sweep found 67 frequency synthesizer parts to be re-marked and falsely sold as new parts. These 67 parts were not installed into an MDA system, but would have been in MDA hardware if they had not been detected as part of the stockroom sweep. Three other MDA counterfeit incidents involved non-mission critical telemetry hardware, resulting in approximately 30 parts being discarded.

Total counterfeit parts found to date number about 1,300. All of them were procured from Unauthorized Distributors. We estimate the total cost to MDA for the seven instances is about $4 million. Our largest case cost the Agency $3 million to remove counterfeit parts discovered in the mission computer of our production THAAD interceptor.

MDA has taken several steps to identify and remove counterfeit parts from within the BMDS supply chain. The Agency:

- Invokes the Parts, Materials, and Processes Mission Assurance Plan (PMAP) on its contracts

- Uses an extensive ground-testing program to identify quality and performance concerns prior to flight
- Supports interagency and Department of Defense efforts to address this problem -- MDA participates in the OSD Anti-Counterfeit Working Group and has shared its internal policies and knowledge base with that group

Remedial actions are considered in each instance and the actions taken necessarily are dependent upon the facts and the responsiveness of the contractors involved.

Although the source of each MDA counterfeit part occurrence was an Unauthorized Distributor, there are circumstances, such as parts obsolescence, that require procurement of parts from an Unauthorized Distributor. Contractors must notify the Program Office with justification and test data in order to purchase any electronic part from an Unauthorized Distributor. MDA performs site assessments of Unauthorized Distributors, pre-flight test reviews and risk assessments of the purchased products from Unauthorized Distributors, and evaluates contractor and subcontractor counterfeit part detection processes. When MDA evaluates an Unauthorized Distributor, we first check prior history, such as memberships in reputable Unauthorized Distributor trade groups. We search for complaints and disputes from other Unauthorized Distributors during the previous two years and review any history we may have with the Unauthorized Distributor. At the Unauthorized Distributor's site, we evaluate their part-level handling for electro-static discharge and environmental controls, inspection and testing capabilities, and training records, to verify that they follow proper procedures and perform sufficient testing to detect possible counterfeits. If the Unauthorized Distributor plans to sell a product to MDA, we evaluate the overall risk based on the criticality of the part.

To date, 51 Unauthorized Distributors have been visited and assessed. Over 50% of the Unauthorized Distributors assessed were viewed as unacceptable by MDA. MDA also has developed part authentication expertise and issues Mission Assurance Advisories and GIDEP (Government Industry Data Exchange Program) alerts to provide program offices and contractors information related to the discovery of new counterfeiting techniques and any specific counterfeit part discovery.

The best time to detect a counterfeit part is at receiving inspection before the part enters production inventories. Robust inspection of parts procured from Unauthorized Distributors is absolutely necessary at receiving inspection. Our experience indicates counterfeit parts are also discovered during end item acceptance testing when electrical stimuli and harsh environments are imposed. However, some counterfeit parts that include the correct die, but are actually used parts, can pass acceptance tests, be fielded and result in a reliability risk.

Due to the early recognition of the counterfeit part problem and the diligence of our contractors, we have been fortunate to identify and limit the cost and schedule impact of counterfeit parts. However, if a counterfeit part is discovered years after it was integrated into the BMDS, recovering the parts through the disassembly of possibly hundreds of operationally deployed systems could be extremely expensive, potentially costing hundreds of millions of dollars. Aside from the financial impacts, the greatest potential impact of counterfeit parts is the operational cost of an interceptor that does not perform as designed when it is needed, a cost that could be measured in lives lost or the negative impacts on foreign policy and national security strategy.

The predominant threat of counterfeit parts in missile defense systems is reduced reliability of a major DoD weapon system. We do not want to be in a position where the reliability of a $12 million THAAD interceptor is destroyed by a $2 part. Among the more significant steps MDA has taken to combat the counterfeit parts risk is establishing requirements in its contracts to provide the pedigree of every single mission critical part used in the BMDS. To date, MDA has had no indication that any mission critical hardware in the fielded BMDS contains counterfeit parts.

Thank you, Mr. Chairman. I look forward to answering the committee's questions.