Testimony of
Vivek Kamath,
Vice President, Supply Chain Operations,
Raytheon Company
before the
United States Senate
Committee on Armed Services
November 8, 2011

Introduction

Mr. Chairman, Ranking Member McCain, members of the Committee, Raytheon appreciates the opportunity to work with you on this important inquiry into counterfeit electronic parts in the Department of Defense (DoD) supply chain. These parts making their way into military equipment pose a real threat to our national security.

Mitigating the risks posed by suspect and counterfeit electronic parts is an issue that Raytheon takes very seriously. It is one of our top priorities. Indeed, our business and our reputation demand this approach, which is why Raytheon spends a great deal of time, resources, and effort tackling this problem on a daily basis.

We are hopeful that the detailed information we have provided to you and your staff throughout the investigation has proven beneficial. I look forward to discussing the proactive steps that Raytheon has taken to combat the threat.

The Challenge of Counterfeit Electronic Parts

According to government and industry data, seven to eight percent of world trade every year involves counterfeit products. Each year, due to counterfeiting, hundreds of thousands of American jobs are lost and U.S. companies lose between $200 and $250 billion.

At Raytheon, we consider an item to be "counterfeit" if it is purposely misrepresented to be genuine. Under this definition, counterfeits include unauthorized or illegal copies, items whose appearance is altered or disguised with the intent to mislead, or items that are refurbished or reclaimed, but advertised as new. Unauthorized substitution of materials or components constitutes counterfeiting under our policies. Raytheon also takes the view that counterfeiting includes falsely advertising that the testing, screening, or qualification of an item is complete.

As in any market, counterfeit electronic parts enter the DoD supply chain because of supply and demand. Rapid turnover in high technology items provides a steady source of used materials that can end up as counterfeit parts. Also, obsolete parts pose a challenge because Original Equipment Manufacturers (OEMs) may have stopped making the parts or left the industry altogether. Despite these challenges,

DoD and its suppliers must obtain the authentic electronic parts needed to build, maintain, and refurbish defense systems.

Counterfeiters are innovative, and their efforts pose a dynamic threat to supply chains. The volume of counterfeit items and rapidly improving methods for concealing them require constant vigilance from all participants in the supply chain. Yet, even with a substantial investment of time and resources by the U.S. government and its suppliers, counterfeit parts will likely continue to find their way into defense and other U.S. government systems. We are fully committed to making sure they do not.

Raytheon Supply Chain Operations

Across Raytheon, our supply chain covers thousands of programs and contracts involving a vast number of suppliers. We issue hundreds of thousands of purchase orders every year. Purchase orders for electronic parts – where the risk of counterfeiting is highest – may cover multiple lots comprised of thousands of individual parts.

As a company, Raytheon is committed to providing genuine electronic parts to our customers. Like others in the industry, Raytheon mandates that suppliers certify, in writing, that the electronic parts they are providing meet the standards in the purchase order – including requirements for authentic parts from authorized sources. In Raytheon's experience, however, the protection afforded by this certification is limited in two principal ways. First, the source information available to suppliers must be reliable. Second, suppliers must be committed to practices designed to mitigate counterfeit electronic parts.

Improving Best Practices

Raytheon has been addressing the presence of counterfeit parts in the supply chain for years. Raytheon's business units operate under policies for detecting and mitigating the risk of counterfeit parts. These policies have protections that reflect the specific needs of each business.

Building on these experiences, we worked with our partners in the defense industry in 2009 to develop SAE Aerospace Standard (AS) 5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition – an industry guideline to develop consistent policies regarding counterfeit parts.

At the same time, Raytheon formed a cross-business team to develop an enterprise-wide counterfeit parts mitigation policy. This policy, which amplifies and integrates existing business practices, was introduced in July 2011 and will be fully implemented in February 2012. Based on SAE AS5553 and Raytheon's own best practices, our counterfeit parts mitigation policy assigns specific responsibilities to Raytheon's Supply Chain Management; Engineering; Mission Assurance; and other functions. The policy also focuses attention on the aspects of our supply chain that are

most likely to present risks, such as the procurement of electronic parts from independent distributors.

To further reduce the possibility that counterfeit parts might find their way into one of our products, Raytheon is developing a Preferred Supplier List for distributors and brokers. This list will allow us to reward suppliers that institute rigorous processes to secure their own supply chains and that have a proven history of supplying us with authentic parts. Limiting our relationships to these responsible suppliers will also allow Raytheon to devote more time to supply chain oversight. In turn, preferred suppliers will have a strong financial incentive to comply with our requirements and standards.

We are also consolidating purchasing across Raytheon through a central procurement organization. All purchases of electronic parts through distributors will be routed through this organization, providing additional governance and oversight of our supply chain.

Like many other organizations in government and industry, Raytheon is a member of the Government - Industry Data Exchange Program (GIDEP). The GIDEP reporting system provides a means for manufacturers and suppliers to alert other GIDEP members when they identify potential counterfeit parts, assemblies, components, and their respective suppliers. This kind of information sharing can help stop suppliers of counterfeit parts in their tracks. Indeed, because of its importance to the security of the entire industry supply chain, Raytheon treats GIDEP reporting as mandatory. Our new enterprise policy will reinforce this practice.

Conclusion

Given the scope and dynamic nature of the threat, counterfeit items will remain a challenge. The policies, practices, and measures that Raytheon has put in place will further protect our supply chain from counterfeit parts, while limiting exposure and mitigating risk for our customers and our company. Effective policy responses will further refine industry best practices and improve information sharing, while avoiding costly or time-consuming solutions that provide little additional protection for the warfighter.

We thank the Committee for focusing its attention on this challenging issue, and I would be happy to answer any questions you may have.